Příloha č. 1a: Technická specifikace

V této příloze jsou uvedeny výchozí podmínky a požadavky na dodávku v rámci této veřejné zakázky.

OBSAH

Obsah 1
Využité zdroje 2
Seznam tabulek 2
Seznam zkratek a pojmů 2
1 Předmět plnění 4
2 Rozsah dodávky a souvisejících služeb 4
2.1 Vymezení předmětu a rozsahu dodávky 4
2.1.1 Související služby a náležitosti dodávky 5
2.1.2 Dodávkou nedotčené oblasti stávajícího řešení 5
2.1.3 Vyloučení z dodávky 5
2.2 Požadavky na dodávky 6
2.2.1 Obecné a společné požadavky 6
2.2.2 Dodávka centrálního systému pro řízení přístupů pracovníků NTa k NIS, LIS a PACS 7
2.2.3 Napojení NIS na centrální systém pro řízení přístupů pracovníků NTa 11
2.2.4 Napojení LIS na centrální systém pro řízení přístupů pracovníků NTa 11
2.2.5 Napojení PACS na centrální systém pro řízení přístupů pracovníků NTa 11
2.2.6 Čtečky karet pro přístup pracovníků NTa k NIS, LIS a PACS 12
2.2.7 Bezpečnostní požadavky 12
2.2.8 Implementační a provozní požadavky 13
2.3 Požadavky na služby 13
2.3.1 Realizace předmětu plnění 13
2.3.2 Seznámení s funkcionalitami, obsluhou dodávaných technologií 15
2.4 Záruky 16
3 Harmonogram 17
4 Místa plnění 18
5 Výchozí stav 19
5.1 Počet uživatelů a pracovních stanic 19
5.2 Stav informačních a komunikačních technologií 19

5.2.1 Datové sítě 19
5.2.2 Ostatní technologie využívané objednatelem 19
Konec dokumentu 21

VYUŽITÉ ZDROJE

Nejsou

SEZNAM TABULEK

Tabulka 1: Seznam zkratek a pojmů 3
Tabulka 2: Předmět a rozsah dodávky 5
Tabulka 3: Obecné a společné požadavky 6
Tabulka 4: Dodávka centrálního systému pro řízení přístupů pracovníků NTa k NIS, LIS a PACS 10
Tabulka 5: Napojení NIS na centrální systém pro řízení přístupů pracovníků NTa 11
Tabulka 6: Napojení LIS na centrální systém pro řízení přístupů pracovníků NTa 11
Tabulka 7: Napojení PACS na centrální systém pro řízení přístupů pracovníků NTa 12
Tabulka 8: Čtečky karet pro přístup pracovníků NTa k NIS, LIS a PACS 12
Tabulka 9: Bezpečnostní požadavky 12
Tabulka 10: Provozní požadavky 13
Tabulka 11: Dokumentace – požadavky na zpracování 14
Tabulka 12: Harmonogram 17
Tabulka 13: Místa plnění 18
Tabulka 14: Počet uživatelů a pracovních stanic 19
Tabulka 15: Datové sítě 19
Tabulka 16: Technologie 21

SEZNAM ZKRATEK A POJMŮ

Zkratka/pojem	Význam
7x24x365	Poskytování služeb 365 dní v roce, 24 hodiny denně, 7 dnů v týdnu
DNS	Domain Name System - hierarchický systém doménových jmen
EU	Evropská unie
FTP	File Transfer Protocol - standardní komunikační protokol pro přenos souborů mezi počítači pomocí počítačové sítě
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob

Zkratka/pojem	Význam
HW	Hardware
IS	Informační systém
JWT	JSON Web Token je navržený internetový standard pro vytváření dat s volitelným podpisem a/nebo šifrováním
LIS	Laboratorní informační systém
MS AD	Microsoft Active Directory
NIS	Nemocniční informační systém
NPS	Implementace serveru RADIUS od fy Microsoft
NTa	Nemocnice Tábor, a.s.
OpenID	Otevřený standard popisující decentralizovaný způsob autentizace uživatelů
OS	Operační systém
PACS	Picture archiving and communication system – technologie umožňující správu, ukládání (archivaci) a zobrazení obrazové dokumentace
PC	Osobní počítač
RADIUS (Accounting)	Remote Authentication Dial In User Service (Uživatelská vytáčená služba pro vzdálenou autentizaci) je AAA protokol používaný pro přístup k síti nebo pro IP mobilitu
RDP	Remote Desktop Protocol - proprietární síťový protokol, který umožňuje uživateli využívat vzdálený počítač prostřednictvím počítačové sítě
SAML	Security Assertion Markup Language - standard založený na XML
SCP	Secure Copy - slouží k bezpečnému přenosu souborů mezi dvěma počítači propojenými počítačovou sítí pomocí protokolu Secure Shell
SIEM	Management bezpečnostních informací a událostí
SNMP (GET)	Simple Network Management Protocol je součástí sady internetových protokolů
SSH	Secure Shell - program a zabezpečený komunikační protokol v počítačových sítích, které používají TCP/IP
SSO	Single Sign-On - jednotné přihlašování uživatelů
SW	Software
VPN	Virtuální privátní síť pro přístup k místní síti

Tabulka 1: Seznam zkratek a pojmů

1 PŘEDMĚT PLNĚNÍ

Předmětem plnění veřejné zakázky (dílem) je komplexní dodávka a implementace technologií, dodávky SW, HW (koncových HW zařízení) pro řízení přístupů pracovníků NTa na pracovní stanice a k NIS, LIS a PACS.

Součástí dodávky budou systémy, aplikace a technologie potřebné k zajištění správy a autentizace všech uživatelů pomocí dvou faktorů, přičemž druhým bude karta, kterou bude možno využít i k dalším účelům, zejména jako bezkontaktní čip pro přístupový systém (Mifare DesFire), průkaz zaměstnance s potiskem a dodávka čteček karet.

Předmět plnění (dílo) je detailně popsán v kap. 2 – Rozsah dodávky a souvisejících služeb.

Servisní služby jsou detailně specifikovány v samostatné příloze.

2 ROZSAH DODÁVKY A SOUVISEJÍCÍCH SLUŽEB

2.1 VYMEZENÍ PŘEDMĚTU A ROZSAHU DODÁVKY

Rozsah dodávky je následující:

#	Položka rozpočtu	Počet	Stručný popis položky
1	Dodávka centrálního systému pro řízení přístupů pracovníků NTa k NIS, LIS a PACS	1 soubor	Dodávka centrálního systému pro řízení přístupů pracovníků NTa (SSO) pomocí karet a řízení přístupů pracovníků NTa na pracovní stanice a k NIS, LIS a PACS, včetně integrace na MS Active Directory. Součástí je vybudování systému, dodávka systému, instalace, zapojení a konfigurace prvků systému a zajištění všech nezbytných integrací (napojení na MS AD, NIS, LIS a PACS atd.). Detailní požadavky jsou uvedeny v kap. 2.2.2.
2	Napojení NIS na centrální systém pro řízení přístupů pracovníků NTa	1 soubor	Dodávka úprav a napojení NIS na centrální systém pro řízení přístupů pracovníků NTa a zajištění SSO na pracovištích, kde je NIS provozován. Součástí je dodávka úprav NIS, instalace, zapojení a zajištění nezbytných integrací na SSO a jeho komponenty. Detailní požadavky jsou uvedeny v kap. 2.2.3.
3	Napojení LIS na centrální systém pro řízení přístupů pracovníků NTa	1 soubor	Dodávka úprav a napojení LIS na centrální systém pro řízení přístupů pracovníků NTa a zajištění SSO na pracovištích, kde je LIS provozován. Součástí je dodávka úprav LIS, instalace, zapojení a zajištění nezbytných integrací na SSO a jeho komponenty. Detailní požadavky jsou uvedeny v kap. 2.2.4.
4	Napojení PACS na centrální systém pro	1 soubor	Dodávka úprav a napojení PACS na centrální systém pro řízení přístupů pracovníků NTa a zajištění SSO na pracovištích, kde je PACS provozován.

#	Položka rozpočtu	Počet	Stručný popis položky
	řízení přístupů pracovníků NTa		Součástí je dodávka úprav PACS, instalace, zapojení a zajištění nezbytných integrací na SSO a jeho komponenty. Detailní požadavky jsou uvedeny v kap. 2.2.5.
5	Čtečky karet pro přístup pracovníků NTa k NIS, LIS a PACS	5 ks	Dodávka USB čteček karet pro RFID čipové karty kompatibilních s technologií Mifare Desfire 13,56 MHz a EM Marine EM4200, 125 kHz a kompatibilních s dodávanými či modernizovanými IS pro přístup pracovníků NTa k NIS, LIS a PACS. Detailní požadavky jsou uvedeny v kap. 2.2.6.

Tabulka 2: Předmět a rozsah dodávky

2.1.1 Související služby a náležitosti dodávky

Součástí dodávky jsou dále následující služby a náležitosti:

1. Projektové řízení dodávky řešení.
2. Zpracování návrhu dodávky a konfigurace dodávaných technologií, související konzultace.
3. Dodávka, implementace, instalace, zapojení a konfigurace dodávaných technologií.
4. Ověření funkčnosti dodaných technologií a jejich (sou)částí.
5. Dodávka dokumentace dodaného vybavení a jeho částí (min. administrátorská dokumentace, dokumentace skutečného provedení/stavu po implementaci, systémová dokumentace). Dokumentace může být jedním dokumentem, nicméně musí obsahovat všechny relevantní informace.
6. Seznámení s obsluhou dodávaného systému a jeho budoucím provozem (správci).
7. Zařazení do provozního prostředí objednatele (dohled, zálohování apod.).
8. Provedení zkušebního provozu.
9. Poskytnutí záruky dodané systémy, technologie a vybavení (viz kap. 2.4).

Služby jsou detailně popsány dále v tomto dokumentu v kap. 2.3, 2.4 a 3.

2.1.2 Dodávkou nedotčené oblasti stávajícího řešení

Dodávkou nebudou negativně dotčeny současné systémy, technologie.

2.1.3 Vyloučení z dodávky

Předmětem dodávky není:

1. Čtečky karet do notebooků a PC nad rámec čteček, které jsou součástí předmětu plnění.
2. Karty uživatelů pro zajištění přístupů zůstanou zachovány.
3. Čtečky karet pro přístupový systém a dveřní systémy napojené na přístupový systém.
4. Zajištění v rámci požadavků neuvedené komunikační infrastruktury (sítě apod.) mezi jednotlivými prvky systému.
5. Infrastruktura, HW a systémový SW poskytované Objednatelem (NTa) uvedené ve výchozím stavu a neuvedené v požadavcích.

Koncept řešení, principy a požadavky na dodávky a služby jsou uvedeny dále v tomto dokumentu.

2.2 POŽADAVKY NA DODÁVKY

V této kapitole jsou uvedeny požadavky na dodávky.

2.2.1 Obecné a společné požadavky

V této kapitole jsou uvedeny obecné požadavky na požadované řešení:

#	Požadavek
P.1	Dodávané technologie musí svojí architekturou splňovat obecné zásady informační bezpečnosti v míře, odpovídající charakteru užití a kategorii zpracovávaných dat (GDPR).
P.2	Veškeré nabízené SW i HW prvky musí být plně kompatibilní se stávajícími systémy a technologiemi NTa uvedenými ve výchozím stavu.
P.3	Součástí implementace musí být i veškeré potřebné licence a služby nezbytné pro dodávku a provoz dodávaných technologií min. po dobu účinnosti servisní smlouvy.
Legislativa a další normy	
P.4	Soulad s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR – General data protection regulation) v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
P.5	Soulad se Zákonem č. 181/2014 Sb., o kybernetické bezpečnosti v aktuálním znění a vyhláškou Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti v aktuálním znění.
P.6	Prováděcí nařízení Komise (EU) 2024/2690 ze dne 17. října 2024, kterým se stanoví pravidla pro uplatňování směrnice (EU) 2022/2555, pokud jde o technické a metodické požadavky na opatření k řízení kybernetických bezpečnostních rizik a bližší upřesnění případů, v nichž se incident považuje za významný, pokud jde o provozovatele DNS, registry domén nejvyšší úrovně, poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, poskytovatele on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí a poskytovatele služeb vytvářejících důvěru
Ostatní obecné požadavky	
P.7	Zajištění jednotného času na všech technologiích a zařízeních (synchronizace s time serverem) .
P.8	Instalace všech dodávaných částí na infrastrukturu poskytovanou objednatelem.
P.9	Kapacita, výkon a licence musí umožnit využívání uživateli a na koncových HW zařízeních dle kap. 5.1.

Tabulka 3: Obecné a společné požadavky

Pro konkrétní oblasti jsou uvedeny specifické požadavky samostatně v dílčích podkapitolách.

2.2.2 Dodávka centrálního systému pro řízení přístupů pracovníků NTa k NIS, LIS a PACS

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
Obecné požadavky	
P.10	Dodávka centrálního systému pro řízení přístupů pracovníků NTa (SSO) pomocí karet a řízení přístupů pracovníků NTa na pracovní stanice a k NIS, LIS a PACS, včetně integrace na MS Active Directory. Součástí je vybudování systému, dodávka systému, instalace, zapojení a konfigurace prvků systému a zajištění všech nezbytných integrací (napojení na MS AD, NIS, LIS a PACS, případně RADIUS server).
P.11	Centrálně spravované parametry: 1. Možnost nastavení doby platnosti zadání hesla uživatele (uživatelské relace/user session). Po tuto dobu lze přistupovat k přihlášené stanici jen s pomocí karty bez nutnosti zadávat znovu heslo. 2. Možnost nastavení doby pro uzamčení při nečinnosti uživatele. Po této době nečinnosti se stanice automaticky uzamkne. 3. Možnost nastavení doby pro odhlášení u uzamčené pracovní stanice. Po této době uzamčení pracovní stanice se stanice automaticky odhlásí, tj. dojde k ukončení aktivní uživatelské relace a aktivních uživatelských procesů, bez ohledu na jejich stav.
P.12	Autentizační systém musí podporovat protokoly SAML, JWT, OpenID, Radius_Accounting a token systém pro integraci řešení třetích stran (integrovaných IS a technologií).
P.13	Auditovat všechny důležité operace: např. přihlášení, odhlášení, zobrazení hesla, přístup přes RDP, přístup do IS, přiřazení karet, výměny karet apod.
P.14	Možnost instalace na serverové OS uvedené ve výchozím stavu (viz kap. 5.2.2).
P.15	Webová aplikace, určená správcům: 1. Přehledy, evidence, správa napojených zařízení a registrovaných uživatelů a karet. 2. Možnost filtrovat a exportovat seznamy/přehledy min. do MS Excel.
P.16	Podpora klientských stanic na platformách MS Windows, MacOS, Linux, iOS a Android.
P.17	Podpora pro webové prohlížeče založené na technologiích Chromium a pro FireFox.
P.18	Předání autentizačních údajů pro RDP, SSH, SCP, FTP, VPN.
P.19	Bezpečné uložení citlivých údajů (hesel, klíčů, certifikátů a souborů) je možné tak, aby uživatelé mohli tyto informace bezpečně sdílet nebo naopak, aby nebyly dostupné nikomu kromě uživatele, který je uložil (ani správci systému, zálohování atd.).
P.20	Řešení má roli Auditora, který si může zobrazit všechny akce provedené uživateli i nad daty, ke kterým sám nemá přístup. Toto zobrazení neumožňuje přístup k datům, pouze k auditním informacím (ty zahrnují identifikaci uživatele, datum, čas a specifikaci místa přístupu – minimálně zdrojovou IP adresu).
P.21	Hromadné načtení dat v rámci dodávky, tj. uživatelů, stanic, skupin, složek apod.

#	Požadavek
Správa uživatelů	
P.22	Správa uživatelů a účtů pro systém: 1. Uživatelské účty – pro přihlášení konkrétních uživatelů k pracovním stanicím nebo do IS 2. Technické účty – pro přihlašování sdílených pracovních stanic. 3. Účty správců – správci / administrátoři systému a pracovních stanic. Všechny účty musí být převzaty a ověřovány vůči doméně MS Active Directory.
P.23	U technických účtů pro sdílené pracovní stanice a účty správců (Administrator) systém automaticky mění heslo každý den. Heslo musí být náhodně generované pro každý účet samostatně a plnit podmínky pro „silné“ heslo. Konfigurace umožňuje nastavení celkové délky hesla a zastoupení znaků (malá/velká písmena, číslice, speciální znaky). Heslo může být zobrazeno správci v systému a jeho zobrazení musí být zaznamenáno do logu / auditu. Zobrazení seznamu uživatelských účtů, které mají hesla, která nejsou v souladu s požadovanými podmínkami.
P.24	Správa skupin uživatelů pro určování kategorií uživatelů, nastavování politik, sdílených složek a přístupů k napojeným IS. Možnost zařazení uživatele do více skupin.
P.25	Správa politik pro uživatele, možnost hromadného přiřazování politik k uživatelům nebo skupinám uživatelů.
P.26	Správa nastavení osobních a sdílených složek, které budou namapovány při přihlášení uživatele. Sdílené složky nastavovat pro skupiny uživatelů.
P.27	Každý uživatel má unikátní osobní číslo, které musí být propagováno napříč systémem a napojenými IS.
P.28	Dvoufaktorová autentizace pro přístup správců do administrace systému: kartou, autentikátory Microsoft a Google.
Správa karet	
P.29	Evidence a správa všech karet, a to jak aktivních, tak neaktivních (historie).
P.30	Možnost zařazení karty do evidence identifikací karty přes čtečku karet.
P.31	Využití stávajících karet (typ viz výchozí stav v kap. 5.2.2).
P.32	Přiřazování karet uživatelům a správcům, změny v přiřazení, výměny apod. Možnost přiřazení více karet jednomu uživateli. V případě přiřazování již přiřazené karty jinému uživateli, upozornit správce a pokud správce akci povolí, tak aktivovat kartu pro nového uživatele a deaktivovat kartu u původního uživatele.
P.33	Možnost dočasného přiřazení karty v případě zapomenutí karty na určenou dobu. Pro přiřazování dočasných karet poskytnout vyhrazenou funkčnost pro stanovené uživatele, kteří nemusí být správci celého systému.

#	Požadavek
P.34	Notifikace správců (emailem) v případě pokusu o přihlášení neaktivními kartami (stanice, uživatel, karta).
Správa stanic	
P.35	Evidence a správa všech napojených pracovních stanic.
P.36	Rozlišení stanic min. na: 1. Sdílené – stanice bude využívána více uživateli, práce více uživatelů je možná pod sdíleným technickým účtem, přiřazení konkrétního sdíleného technického účtu pro přihlášení stanice. 2. Nesdílené – stanice bude využívána jen identifikovanými uživateli, práce je možná jen pod účtem konkrétního registrovaného uživatele.
P.37	Rozdělení stanic do skupin pro snadnější rozlišení jejich umístění, typu, specifických parametrů / nastavení.
P.38	Správa politik pro pracovní stanice, možnost hromadného přiřazování politik ke stanicím nebo skupinám stanic.
P.39	Možnost přiřazení technického účtu více pracovním stanicím nebo skupině stanic.
Správa oprávnění do napojených informačních systémů	
P.40	Správa napojených IS, kterým bude poskytována služba SSO, včetně nezbytné konfigurace, technických účtů pro integraci apod. Ve výchozím stavu provedení nastavení min. pro LIS, NIS a PACS.
P.41	Správa oprávnění uživatelů pro přihlášení do vybraných napojených IS. Možnost hromadného nastavení uživatelům nebo skupinám uživatelů.
P.42	Možnost přebírání oprávnění uživatelů pro přístup do IS z MS Active Directory.
Funkcionality na pracovních stanicích	
P.43	Instalace agentů / komponent na pracovní stanice, které budou zajišťovat funkcionality a služby pro pracovní stanice (OS) a instalované IS a technologie.
P.44	Spuštění pracovní stanice: 1. Sdílené pracovní stanice – automaticky se přihlásí pod sdíleným technickým účtem a uzamkne se do doby přihlášení konkrétního uživatele pod svým osobním uživatelským účtem. 2. Nesdílené pracovní stanice – přihlášení musí provést uživatel pod svým osobním uživatelským účtem.
P.45	Přihlášení uživatele proběhne s využitím načtení uživatelské karty přes čtečku a zadání hesla z domény MS Active Directory. Přihlášení proběhne nejpozději do 10 s.
P.46	Aktualizace politik pracovních stanic a uživatelů a nastavení složek (osobních i sdílených) při přihlášení uživatele dle nastavení v centrální části systému (pracovní stanice dle technického nebo uživatelského účtu, prostředí uživatele dle přihlášeného uživatele).

#	Požadavek
P.47	Po prvním zadání hesla na dané stanici je toto heslo zapamatováno po konfigurovatelnou dobu – v této době může uživatel zamykat, odemykat a střídat se s jinými uživateli pouze použitím své karty.
P.48	Možnost přihlášení správcem pod účtem Administrator pod heslem zjištěným z centrální části systému.
P.49	Uzamčení nebo odhlášení dle podmínek v požadavku P.11.
P.50	Integrované systémy na pracovních stanicích: 1. V rámci přihlašování do systému předávat token aktuálně přihlášeného uživatele. 2. Při odhlášení uživatele předávat informaci o odhlášení uživatele.
P.51	Možnost přístupu na vzdálené plochy (RDP) stanic a serverů po zadání hesla.
Integrace na MS Active Directory	
P.52	Přebírání a aktualizace uživatelů z MS Active Directory, včetně zařazení do skupin a relevantních uživatelských dat (osobní číslo, jméno, příjmení, funkce apod.).
P.53	Ukončování přístupů uživatelů, kteří mají ukončenu platnost uživatelského účtu v MS AD.
P.54	Dle zařazení uživatelů do skupin automaticky nastavovat oprávnění pro napojené IS: NIS, LIS a PACS. Nastavení skupin bude definováno v rámci dodávky.
Integrační rozhraní pro IS a technologie	
P.55	Dodávka integračního rozhraní (API) pro napojení IS nebo technologií pro ověřování oprávnění přístupu uživatelů do daného IS. Poskytnutí dokumentace a příkladů pro ověření a řešení problémů s napojením.
P.56	Možnost napojení jen registrovaného IS dle požadavku P.40.
P.57	Poskytování tokenů pro ověřování uživatelů v napojeném IS.
Ostatní požadavky	
P.58	Možnost integrace dvoufaktorové autentizace na RADIUS server v rámci domény MS Windows. Implementace pro Access přístup pomocí RADIUS serveru (Microsoft NPS) s využíváním atributů protokolu RADIUS (závislé podle dodavatele – AV-Pair apod.) pro jednotlivé skupiny uživatelů AD. Integrace bude realizována, pokud bude RADIUS server připraven v době dodávky. Pokud nebude připraven, bude napojení realizováno v rámci servisních služeb na vyžádání.
Dodávka / instalace	
P.59	Instalace, zapojení a konfigurace systému. *Provozní infrastrukturu poskytne objednatel.*
P.60	Veškerá nastavení a oprávnění musí být v souladu se zákonnými požadavky na ochranu osobních údajů.

Tabulka 4: Dodávka centrálního systému pro řízení přístupů pracovníků NTa k NIS, LIS a PACS

2.2.3 Napojení NIS na centrální systém pro řízení přístupů pracovníků NTa

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.61	Napojení NIS na centrální systém pro řízení přístupů pracovníků NTa: 1. Napojení na evidenci uživatelů v centrálním systému a přebírání potřebných údajů o uživatelích. 2. Přihlašování do IS přes komponentu SSO na pracovních stanicích zajišťující ověření uživatele přes kartu a heslo. V případě, že platnost ověření hesla nevypršela, přihlášení bez nutnosti zadat heslo. Neumožnit přihlášení uživateli, který nemá platný a ověřený účet v SSO. 3. Přebírání informace o odhlášení uživatele z komponenty SSO na pracovních stanicích.
P.62	V případě přepnutí uživatele v komponentě SSO provést odhlášení původního uživatele a přihlášení nového uživatele. Pokud systém disponuje funkcí přepínání účtů, lze využít tuto funkcionalitu místo odhlášení / přihlášení.

Tabulka 5: Napojení NIS na centrální systém pro řízení přístupů pracovníků NTa

2.2.4 Napojení LIS na centrální systém pro řízení přístupů pracovníků NTa

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.63	Napojení LIS na centrální systém pro řízení přístupů pracovníků NTa: 1. Napojení na evidenci uživatelů v MS Active Directory a přebírání potřebných údajů o uživatelích. 2. Přihlašování do IS přes MS AD na pracovních stanicích zajišťující ověření uživatele přes doménu MS AD. V případě, že platnost ověření hesla nevypršela, přihlášení bez nutnosti zadat heslo. Neumožnit přihlášení uživateli, který nemá platný a ověřený účet v MS AD. 3. Přebírání informace o odhlášení uživatele z komponenty MS AD na pracovních stanicích.
P.64	Pro přepnutí uživatele provést odhlášení původního uživatele a přihlášení nového uživatele dle předchozího požadavku. Pokud systém disponuje funkcí přepínání účtů, lze využít tuto funkcionalitu místo odhlášení / přihlášení.

Tabulka 6: Napojení LIS na centrální systém pro řízení přístupů pracovníků NTa

2.2.5 Napojení PACS na centrální systém pro řízení přístupů pracovníků NTa

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.65	Napojení PACS na centrální systém pro řízení přístupů pracovníků NTa: 1. Napojení na evidenci uživatelů v centrálním systému a přebírání potřebných údajů o uživatelích.

#	Požadavek
	2. Přihlašování do IS přes komponentu SSO na pracovních stanicích zajišťující ověření uživatele přes kartu a heslo. V případě, že platnost ověření hesla nevypršela, přihlášení bez nutnosti zadat heslo. Neumožnit přihlášení uživateli, který nemá platný a ověřený účet v SSO. 3. Přebírání informace o odhlášení uživatele z komponenty SSO na pracovních stanicích.
P.66	V případě přepnutí uživatele v komponentě SSO provést odhlášení původního uživatele a přihlášení nového uživatele. Pokud systém disponuje funkcí přepínání účtů, lze využít tuto funkcionalitu místo odhlášení / přihlášení.

Tabulka 7: Napojení PACS na centrální systém pro řízení přístupů pracovníků NTa

2.2.6 Čtečky karet pro přístup pracovníků NTa k NIS, LIS a PACS

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.67	Dodávka USB čteček karet pro RFID čipové karty kompatibilních s technologií Mifare Desfire 13,56 MHz a EM Marine EM4200, 125 kHz a kompatibilních s dodávanými či modernizovanými IS pro přístup pracovníků NTa k NIS, LIS a PACS.

Tabulka 8: Čtečky karet pro přístup pracovníků NTa k NIS, LIS a PACS

2.2.7 Bezpečnostní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.68	Autorizace: Poskytnutí přístupu autentizovaného uživatele k aktivu systému (data, aplikace), odpovídající pracovnímu zařazení uživatele a přidělené roli (rolím) v systému. Systém umožní řídit přístupová oprávnění jednotlivých subjektů jen k údajům, ke kterým mají a mohou mít přístup.
P.69	Zabránění vstupu neautorizovaného subjektu do systému – zamezení možnosti přístupu neoprávněného subjektu.
P.70	Zajištění šifrované komunikace mezi všemi součástmi systému a pracovišti uživatelů, případně zajištění komunikace v odděleném síťovém prostředí.
P.71	Evidence přístupů všech uživatelů do systémů a technologií (logování) včetně časových údajů.
P.72	Veškeré přístupy k datům a aktivita uživatelů v rámci dodávaných systémů a technologií budou logovány tak, aby byly zřejmé přístupy k jednotlivým údajům a zpětná kontrola těchto údajů.
P.73	Veškeré logy budou dostupné pro externí systém sběru a analýzy logů. Podpora přenosu dat do SYSLOG / SIEM.

Tabulka 9: Bezpečnostní požadavky

2.2.8 Implementační a provozní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.74	Všechny komponenty musí být připraveny na provoz 24x7x365 (non-stop).
P.75	Předmětem zakázky jsou i veškeré služby související s dodávkou – doprava, instalace, implementace do stávající infrastruktury, konfigurace a zprovoznění komunikace, nastavení datových toků, seznámení s obsluhou a správou systému, testování. Veškeré seznámení s obsluhou bude probíhat v prostorách objednatele a v českém jazyce. Součástí nabídkové ceny musí být i veškeré práce či činnosti, které v této zadávací dokumentaci nejsou explicitně uvedeny, ale které musí dodavatel s ohledem na jím nabízený předmět veřejné zakázky a jeho řádnou a úplnou realizaci provést k dosažení objednatelem požadovaného cílového stavu.
P.76	Instalace do prostředí objednatele uvedeného v kap. 5.2 – Stav informačních a komunikačních technologií.
P.77	V rámci implementace musí dodavatel zajistit plnohodnotný provoz dodávaného řešení současně s provozem stávajících systémů a technologií. To vše s minimálním omezením provozu. Dodavatel je povinen přizpůsobit realizaci předmětu zakázky podmínkám objednatele.
P.78	Zajištění administrátorských aplikací, konzolí pro všechny součástí systému pro zajištění konfiguračního managementu systému anebo jeho součástí.
P.79	Dohled – dodávané systémy a technologie musí předávat informace o svém stavu (stavu služeb apod.) na žádosti SNMP GET. Zhotovitel poskytne parametry, podmínky a součinnost při nastavení dohledu dodaného řešení.
P.80	Synchronizace času všech zařízení s time serverem nebo zprostředkovaně přes centrální systém.
P.81	Pro případ nedostupnosti systému v případě výpadku systém umožní náhradní způsob přístupu uživatelů k aktivům a systémům. Náhradní způsob budou moci aktivovat správci na základě udělených oprávnění.

Tabulka 10: Provozní požadavky

2.3 POŽADAVKY NA SLUŽBY

2.3.1 Realizace předmětu plnění

Součástí předmětu plnění je zajištění služeb souvisejících s realizací předmětu plnění minimálně v následujícím rozsahu:

1) Objednatel požaduje před zahájením implementačních prací zpracování **Implementační analýzy včetně návrhu řešení** (konkretizace implementačního postupu, přesné konfigurace a instalačního a montážního návrhu řešení z nabídky), která bude zahrnovat informace pro všechny aktivity potřebné pro řádné zajištění implementace a montáže předmětu plnění. Implementační analýza včetně návrhu řešení musí být před zahájením prací schválena objednatelem. Implementační analýza včetně návrhu řešení musí zohlednit podmínky stávajícího stavu a požadavky cílového stavu.

2) **Zajištění projektového vedení/řízení** realizace předmětu plnění ze strany zhotovitele a jeho případných poddodavatelů.
3) **Vývoj, implementace a nastavení** informačních a komunikačních technologií odpovídající schválenému návrhu řešení uvedenému v Implementační analýze a příprava pro ověření ze strany objednatele a součinnost pro ověření na straně Objednatele.
4) **Dodávka předmětu plnění**. Součástí dodávky musí být instalace, upgrade a sestavení předmětu zakázky včetně:
   a) Instalace a nastavení SW budou provedeny kvalifikovanými osobami pro dané typy zařízení
   b) Nastavení SW aplikací
5) **Zajištění instalace všech součástí dodávky** v určených lokalitách a prostorách objednatele.
6) **Zajištění instalace a připojení** k zařízením a technickým prostředkům zajištěným objednatelem.
7) **Realizace pilotního provozu** k ověření funkčnosti systému na menším obejmu dat, s menším počtem uživatelů a na menším počtu zařízení.
8) **Převedení systémů do zkušebního provozu** a plná podpora uživatelů v rámci zkušebního provozu včetně technické podpory. V této etapě budou realizována požadovaná seznámení s funkcionalitami, obsluhou dodávaného zařízení a budoucím provozem.
9) **Zpracování dokumentace skutečného provedení, systémové/provozní dokumentace, projektové dokumentace a uživatelské dokumentace** – součástí předmětu plnění je zajištění systémové a provozní dokumentace související s realizací předmětu plnění minimálně v následujícím rozsahu:

Název	Popis
Uživatelská dokumentace	Bude popisovat konkrétní funkčnost z pohledu uživatele tak, aby byl uživatel schopen práce s informačním systémem a pochopil význam jednotlivých částí systému a vazeb mezi nimi. V uživatelské příručce bude popisován způsob práce s jednotlivými částmi systému, vazby mezi nimi včetně popisu součástí jednotlivých částí systému. K usnadnění práce bude sloužit popis jednotlivých obrazovek, ovládacích prvků na obrazovkách a jejich významů, který bude uveden v rámci uživatelské dokumentace.
Dokumentace skutečného provedení a systémová/provozní dokumentace	Obsahuje popis informačního systému (rozhraní a služby) včetně popisu správy informačního systému, definování uživatelů, jejich oprávnění a povinností a detailní popis údržby systému. Pro případ nedostupnosti systému v případě výpadku bude součástí dokumentace postup pro zajištění náhradního způsobu přístupu uživatelů k aktivům a systémům.
Projektová dokumentace	Smluvní dokumentace, harmonogram realizace projektu, analýzy. a prováděcí projekty, zápisy z jednání, protokoly (předávací, akceptační).

Tabulka 11: Dokumentace – požadavky na zpracování

Dokumentace bude dodána v relevantním rozsahu na všechna místa plnění projektu.

Dokumentace bude v souladu se zákonem č. 365/2000 Sb. o informačních systémech veřejné správy a prováděcích právních předpisů, v platném znění.

Dokumenty budou zpracovávány v následujících programech elektronicky a uloženy v následujících formátech:

- MS Office 2016 (MS Word 2016, MS Excel 2016, MS PowerPoint 2016)
- MS Project 2016
- WinZip (formát .zip)
- Portable Document Format (formát .pdf).

Preferovaná forma předávaných dokumentů, které nebudou vyžadovat podpisy konkrétních osob je elektronicky, a to na elektronických nosičích (CD, DVD, flash disk apod.). K předávání a k archivaci souborů se používají média s možností pouze zápisu, nikoliv přepisovatelná.

Veškerá dokumentace bude podléhat schvalování (akceptaci) při převzetí ze strany objednatele.

Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána ve 2 kopiích v elektronické formě ve standartních formátech (MS Office a PDF) používaných objednatelem na datovém nosiči, listinná forma se nepožaduje.

10) **Provedení akceptačních testů.** Zhotovitel je povinen kompletně připravit podklady pro akceptaci dodaného řešení. Součástí akceptace bude akceptační protokol a kompletní předávací dokumentace.
11) **Uvedení systému do produkčního provozu**, zajištění potřebných nastavení a přístupů pro všechny pracovníky objednatele, minimalizace dopadů na provoz objednatele při přechodu a zvýšená podpora bezprostředně po přechodu do produkčního provozu.
12) Zhotovitel dle svého uvážení doplní v nabídce další služby, které jsou dle jeho názoru nezbytné pro úspěšnou realizaci zakázky.
13) Veškeré náklady na zajištění služeb souvisejících s realizací předmětu plnění musí být zahrnuty v ceně odpovídající části předmětu dodávky.

2.3.2 Seznámení s funkcionalitami, obsluhou dodávaných technologií

V této kapitole jsou uvedeny požadavky na seznámení s funkcionalitami, obsluhou dodávaných technologií a jejich budoucím provozem:

1) Zhotovitel proškolí pracovníky objednatele se všemi typy dodaných zařízení a aplikací a problematikou jejich užití, provozu a obsluhy. Zhotovitel se zavazuje poskytnout informace minimálně k následujícím tématům v dostatečném detailu pro porozumění činnosti zařízení a způsobu provozu:
    a) Základní produktové seznámení s jednotlivými dílčími technologickými celky.
    b) Celkové schéma součinnosti jednotlivých zařízení a jejich návaznosti.
    c) Obsluha jednotlivých dílčích modulů, aplikací a technologických celků
    d) Použitá nastavení zařízení, detailnější rozbor použitých konfigurací.
    e) Základní kroky správy, diagnostiky a elementární postupy pro řešení problémů.
2) Poskytnuté informace zajistí seznámení pracovníků objednatele se všemi podstatnými částmi dodávky v rozsahu potřebném pro obsluhu, provoz, údržbu a identifikaci nestandartních stavů systému a jejich příčin.
3) Vše uvedené bude probíhat v prostorách objednatele s využitím vybavení dodaného v rámci této veřejné zakázky, případně zajištěné ze strany objednatele.
4) Konkrétní termíny určí objednatel dle postupu v rámci realizace projektu a dostupnosti zainteresovaných osob.
5) Seznámení s funkcionalitami, obsluhou dodávaných technologií se týká správců.

Veškeré náklady na zajištění těchto činností musí být zahrnuty v ceně odpovídající části předmětu dodávky.

2.4 ZÁRUKY

V této kapitole jsou uvedeny požadavky na záruky dodávky jako celku, případně specificky dílčích částí dodávky.

Objednatel požaduje záruku na veškeré dodané technologie v délce trvání minimálně:

1. 60 měsíců – na informační systémy a SW technologie.
2. 24 měsíců – na koncová HW zařízení (čtečky).

Záruka začíná běžet od okamžiku předání do ostrého (produkčního) provozu. Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele (objednatele). Veškeré komponenty a práce budou poskytnuty bezplatně v rámci záruky. Zhotovitel ve své nabídce výslovně uvede všechny podmínky záruk nad rámec požadavků zadávací dokumentace.

a) Po dobu záruky na části dodávky musí zhotovitel nebo výrobce všech zařízení garantovat běžnou dostupnost náhradních komponentů a dostupnost servisu a opravných balíčků.
b) On-line přístup k aktualizacím software.
c) Součástí záruky je i shoda dodávaných systémů s platnou legislativou.
d) Max. doba na odstranění vady díla je 30 dnů od prokazatelného oznámení dodavateli.
e) Zhotovitel uvede provozní služby požadovaného předmětu plnění veřejné zakázky včetně parametrů, které budou součástí provozu v rámci záruky systému.

3 HARMONOGRAM

Následující tabulka obsahuje požadovaný časový harmonogram realizace dodávky (T ~ datum účinnosti smlouvy o dílo):

#	Fáze	Doba trvání od zahájení	Doplňující informace
1	Zahájení realizace	0	Zahájení realizace bude dnem podpisu smlouvy na dodávku.
2	Analýza a návrh řešení	30	Zpracování analýzy a návrhu řešení pro potřeby upřesnění podmínek realizace.
3	Dodávka, implementace, instalace, konfigurace SW	90	Dodávka, implementace, instalace, konfigurace SW.
4	Vývoj a implementace úprav SW, dodávka dokumentace k SW.	90	Vlastní vývoj a implementace úprav IS dle analýzy a návrhu řešení.
5	Ověření funkčnosti dodaných technologií a systémů.	120	Otestování funkčnosti technologií a systémů a ověření jejich plné funkčnosti.
6	Seznámení s funkcionalitami, obsluhou dodávaných technologií	120	Seznámení s funkcionalitami, obsluhou dodávaných technologií
7	Dodávka dokumentace dodaného systému a jeho částí.	120	Min. uživatelská dokumentace, dokumentace skutečného provedení, systémová/provozní dokumentace, projektová dokumentace.
8	Převedení do zkušebního provozu.	120	Převedení do zkušebního provozu, odstranění všech vad a nedodělků.
9	Ukončení realizace dodávky	180	Součástí je dokončení realizace a převedení do ostrého provozu, zahájení doby provozu dodaného systému a poskytování servisních služeb.

Tabulka 12: Harmonogram

Doplňující informace:

- Pod pojmem „den“ je míněn kalendářní den.
- Zhotovitel má možnost definovat kratší termíny plnění (v rámci dodávky), v nabídce nelze zkrátit dobu zkušebního provozu, která musí být minimálně 60 dnů.
- Zkrácení zkušební doby je možné pouze na základě písemné dohody se Zadavatelem.

4 MÍSTA PLNĚNÍ

Realizace předmětu plnění bude probíhat v následujících místech plnění:

Místo	Adresa	Předmět realizace
Sídlo a centrální datové centrum	kpt. Jaroše 2000, Tábor PSČ: 390 03	Datové centrum NTa: dodávka částí technologie. Sídlo NTa: místo předání výstupů projektu. Pracoviště uživatelů NTa: místo pro provozování systému, dodávka částí technologie.

Tabulka 13: Místa plnění

5 VÝCHOZÍ STAV

V této kapitole je uveden výchozí stav a výchozí podmínky pro dodávku předmětu plnění.

5.1 POČET UŽIVATELŮ A PRACOVNÍCH STANIC

V následující tabulce je uveden počet uživatelů a pracovních stanic:

Kategorie	Počet
Počet uživatelů (uživatelských účtů):	1 000
Počet pracovních stanic:	670
Počet technických účtů pro sdílené stanice:	400

Tabulka 14: Počet uživatelů a pracovních stanic

5.2 STAV INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ

V této kapitole je uveden základní popis výchozího stavu jednotlivých prvků ostatních informačních a komunikačních technologií.

5.2.1 Datové sítě

V rámci projektu budou využity následující sítě:

Datová síť	Popis
WAN	Bude využita pro komunikaci mezi pracovišti uživatelů a centrálními částmi systému z důvodu nutné výměny dat souvisejících s realizací a provozem projektu.
WiFi	Bude využita pro komunikaci mezi pracovišti uživatelů a centrálními částmi systému z důvodu nutné výměny dat souvisejících s realizací a provozem projektu.

Tabulka 15: Datové sítě

5.2.2 Ostatní technologie využívané objednatelem

Objednatel využívá následující technologie. Ve vybraných případech tyto technologie definují prostředí, pro které je dodávka díla požadována:

Oblast	Technologie	Doplňující informace
Pracovní a klientské stanice uživatelů	MS Windows 11 (32 i 64 bit) MS Edge, Chrome, Firefox Procesor: Intel Core i3 10th gen. a vyšší Paměť: 8GB RAM a více Úložiště: 240 GB SSD a více	Informační systémy a technologie pro uživatele musí být funkční na těchto technologiích.
Operační systémy na serverech	Objednatel provozuje systémy na OS MS Windows (Datacenter 2019 R2 a 2022) a Linux	Zadavatel požaduje v rámci dodávky daný SW v aktuální verzi a potřebném počtu k dodávanému SW.

Oblast	Technologie	Doplňující informace
Správa uživatelů	MS Active Directory	Objednatel využívá pro autentizaci Active Directory se stromovou i doménovou úrovní Windows Server 2019 s plánovaným přechodem na 2022. Objednatel poskytne přístup k tomuto systému pro propojení a případná nastavení.
Dohled	Zabbix	Zhotovitel poskytne vstupy pro dohled nad během systému jako celku.
Vzdálený přístup	VPN	Konkrétní typ a podmínky využití budou poskytnuty v rámci součinnosti K čemuž bude uzavřena vzájemná smlouva o vzdáleném přístupu. Vzdálený přístup pro management prostředí bude umožněn pomocí VPN objednatele.
Databáze	Objednatel využívá databázové technologie MS SQL	Zadavatel preferuje v případě dodávky daný SW.
Patch Management	MS WSUS server, MS Systém Center Endpoint Manager	Patch management je řešen ze strany interních aktualizačních serverů a provádí se s týdenním až dvoutýdenním zpožděním kvůli otestování případných problémů, které mohou způsobit hotfixy a bezpečnostní záplaty.
Karty	Mifare Desfire	Bezkontaktní RFID čipová karta kompatibilní s technologií EM Marine EM4200, 125 kHz (bez čipu). Systém musí být kompatibilní a pracovat s těmito kartami.
Čtečky karet	Nejsou	Zadavatel nedisponuje čtečkami karet, čtečky jsou součástí dodávky.
Přístupový systém	IVAR	Přístupový systém bude využívat stejné karty, ale systémy nebudou propojeny.
Nemocniční informační sytém	Dodavatel STAPRO s.r.o. Produkt: FONS Akord	Dodávka úprav a napojení NIS na centrální systém pro řízení přístupů pracovníků NTa a zajištění SSO. Systém musí zůstat zachován.
Laboratorní informační systém	Dodavatel STAPRO s.r.o. Produkt: FONS OpenLIMS	Dodávka úprav a napojení LIS na centrální systém pro řízení přístupů pracovníků NTa a zajištění SSO. Systém musí zůstat zachován.

Oblast	Technologie	Doplňující informace
PACS	Dodavatel: OR-CZ spol. s r.o. Produkt: MARIE PACS	Dodávka úprav a napojení PACS na centrální systém pro řízení přístupů pracovníků NTa a zajištění SSO. Systém musí zůstat zachován.

Tabulka 16: Technologie

V případě neuvedení oblasti objednatel nespecifikuje technologii, případně podmínky pro její použití.

KONEC DOKUMENTU