

Servisní smlouva

uzavřená dle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „**občanský zákoník**“), mezi těmito smluvními stranami:

Uherskohradišťská nemocnice a.s.

sídlo: J. E. Purkyně 365, 686 06 Uherské Hradiště

IČ: 27660915, DIČ: CZ27660915

zápis v obchodním rejstříku: Krajský soud v Brně oddíl B, vložka 4420

zastoupení: MUDr. Petr Sládek, předseda představenstva

(dále jen „**Objednatel**“) na straně jedné

a

Siemens Healthcare, s.r.o.

sídlo: Budějovická 779/3b, 140 00 Praha 4

IČ: 04179960, DIČ: CZ04179960

zápis v obchodním rejstříku: u Městského soudu v Praze, oddíl C, vložka 243136

zastoupení: Mgr. Michal Čech a Ing. Karel Kopejtko, jednatele

číslo účtu: [REDACTED]

kontaktní osoby: [REDACTED]

telefon, e-mail: [REDACTED]

(dále jen „**Poskytovatel**“) na straně druhé

a to v následujícím znění:

I. ÚČEL SMLOUVY

- I.1** Účelem této smlouvy je poskytování pozáručního servisu, provádění neplánovaných oprav a dalších činností pro zdravotnický prostředek Objednatele tak, aby jej Objednatel mohl řádně a nerušeně používat v souladu s jeho účelovým určením, v souladu s právními předpisy a dalšími podmínkami, kterými je Objednatel povinen se při používání tohoto zdravotnického prostředku řídit, jakož i v souladu se zadávací dokumentací na veřejnou zakázku „Pozáruční full servis pro mamograf MAMMOMAT Inspiration“ (dále jen „Zadávací dokumentace“ a „Veřejná zakázka“).

II. PŘEDMĚT SMLOUVY

- II.1** Poskytovatel je s odbornou péčí profesionála a za podmínek této smlouvy a Zadávací dokumentace povinen poskytovat pozáruční servis pro zdravotnický prostředek Objednatele, kterým je mamografický RTG přístroj MAMMOMAT Inspiration s v. č. 50101, (dále též jen „**Zařízení**“). Objednatel je povinen za pozáruční servis za podmínek této smlouvy Poskytovateli hradit sjednanou cenu.
- II.2** Pozáručním servisem se rozumí provádění následujících činností (dále jen „**servisní úkony**“), přičemž obsah těchto činností se vykládá ve smyslu obecně závazných právních předpisů, zejména dle zákona č. 375/2022 Sb., o zdravotnických prostředcích a diagnostických prostředcích in vitro (dále ZoZP). Servisní úkony neupravené v ZoZP se vykládají dle této smlouvy a dle dokumentace výrobce k Zařízení.
- II.3** Poskytovatel je rovněž povinen za podmínek této smlouvy Objednateli řádně a včas dodávat náhradní díly k Zařízení a převádět na Objednatele vlastnické právo k těmto náhradním dílům. Objednatel je povinen řádně, včas a za podmínek této smlouvy dodané náhradní díly převzít a zaplatit za ně Poskytovateli příslušnou cenu.
- II.4** Servisními úkony se rozumí zejména:
- a) Pravidelné servisní prohlídky podle technické dokumentace výrobce, včetně nákladů na práci a cestovného, provedení bezpečnostně technické kontroly dle ZoZP a periodické elektorevize, Interval servisních prohlídek je 6 měsíců.
 - b) Servisní pohotovost
Poskytovatel je povinen zahájit odstraňování závady:
 - (i) do 1 pracovního dne, pokud byla závada nahlášena v pracovní den v době 8-16 hod SEČ;
 - (ii) do 2 pracovních dnů, pokud byla závada nahlášena v jiné době než v pracovní den 8-16 hod SEČ.Kontaktní údaje pro nahlášení závady jsou:
e-mail: servis.cz@siemens-healthineers.com Tel: 800 888 910
- Poskytovatel je povinen odstranit závadu nejpozději:
- (iii) do 2 pracovních dnů od uplynutí doby pro zahájení odstraňování závady v případě, kdy není třeba dodat náhradní díl zahraničního dodavatele;
 - (iv) do 5 pracovních dnů od uplynutí doby pro zahájení odstraňování závady v případě, kdy je třeba dodat náhradní díl zahraničního dodavatele.
- c) Technická podpora vzdáleným přístupem
 - d) Telefonická podpora uživatelů bez omezení času
 - e) Aplikační podpora, školení uživatelů
 - f) Aktualizace softwaru přístroje
 - g) Náklady na opravu provedenou na místě bez náhradních dílů (práce, cestovné)
 - h) Náhradní díly použité při opravách
 - i) Zkoušky dlouhodobé stability
 - j) Elektro-revize Zařízení

II.5 Servisní úkony dle čl. II.4 a), i) a j)..... je Poskytovatel povinen provádět i **bez vyzvání**.

III. OBECNÉ PODMÍNKY PROVÁDĚNÍ SERVISU

- III.1** Poskytovatel je povinen při plnění svých povinností podle této smlouvy respektovat provozní podmínky a pokyny Objednatele. Objednatel je povinen v rámci svých možností učinit všechna opatření k ochraně Zařízení před neoprávněnými zásahy, zejména pak omezit okruh osob, které mají k Zařízení přístup, zejména na osoby proškolené, a to za účelem minimalizace nevhodného zásahu do Zařízení.
- III.2** Poskytovatel je povinen poskytovat služby ve vysoké kvalitě, odpovídající zadávacím podmínkám Objednatele a jeho oprávněným očekáváním. Poskytovatel se zavazuje poskytovat služby kvalifikovanými pracovníky, kteří jsou vyškoleni výrobcem zařízení, vlastní certifikáty vydané jim výrobcem, dle platných předpisů a norem.
- III.3** Poskytovatel bere na vědomí, že servis zdravotnického prostředku může vykonávat pouze právnická nebo podnikající fyzická osoba registrovaná Státním ústavem pro kontrolu léčiv jako osoba provádějící servis. Jde-li o zdravotnický prostředek s měřicí funkcí, musí být jeho servis vykonáván v souladu s jiným právním předpisem upravujícím oblast metrologie.

IV. PROVÁDĚNÍ SERVISNÍCH ÚKONŮ A OPRAV

- IV.1** Není-li výslovně sjednáno jinak, bude vzájemná komunikace smluvních stran probíhat e-mailem.
Kontaktní údaje Poskytovatele jsou následující:

e-mail: servis.cz@siemens-healthineers.com

tel: 800 888 910

Kontaktní údaje Objednatele jsou:

e-mail: [REDACTED]

tel.: [REDACTED]

Za podmínek této smlouvy probíhá komunikace telefonicky.

- IV.2** Nejméně dva pracovní dny před každou plánovanou opravou nebo provedením servisního úkonu, které je Poskytovatel povinen provést i bez vyzvání, je Poskytovatel povinen zaslat Objednateli písemnou informaci o záměru provést plánovanou opravu nebo takový servisní úkon.
- IV.3** O provedeném servisním úkonu a o provedené opravě je Poskytovatel povinen vyhotovit písemný protokol, který je Poskytovatel povinen předat Objednateli bez zbytečného odkladu, nejpozději však **do 5 kalendářních dnů**, po provedení servisního úkonu.
- IV.4** Pokud je Poskytovatel podle této smlouvy pro splnění Objednávky povinen dodat náhradní díly, sepíší smluvní strany písemný předávací protokol o řádném dodání takových náhradních dílů podepsaný oběma smluvními stranami.

V. CENA A PLATEBNÍ PODMÍNKY

- V.1** Objednatel se zavazuje platit Poskytovateli za provádění servisních úkonů, včetně dodání náhradních dílů, cenu - servisní paušál - ve výši

49 250,00 Kč (bez DPH) za měsíc

Za dobu trvání smlouvy 6 let tak Objednatel uhradí Poskytovateli celkovou cenu ve výši

3 546 000,00 Kč (bez DPH).

Součástí uvedené ceny (servisního paušálu) jsou veškeré náklady Poskytovatele spojené s plněním dle této smlouvy.

- V.2** Objednatel se za podmínek této smlouvy zavazuje hradit cenu za provádění servisních úkonů (měsíční paušál) na základě měsíčních faktur – daňových dokladů vystavovaných Poskytovatelem vždy k poslednímu dni kalendářního měsíce, za který je cena hrazena. Faktura musí splňovat veškeré náležitosti daňového a účetního dokladu stanovené právními předpisy. Splatnost faktury se sjednává na 30 dnů od doručení faktury Objednateli. Poskytovatel je povinen zaslat Objednateli fakturu v elektronické podobě ve formátu PDF nebo ISDOC na e-mail: *financni@nemuh.cz*

- V.3** Úhrady cen budou prováděny bezhotovostními převody z bankovního účtu Objednatele na bankovní účet Poskytovatele. Dnem úhrady se rozumí den odepsání příslušné částky z účtu Objednatele.

- V.4** V případě, že v okamžiku uskutečnění zdanitelného plnění bude Poskytovatel zapsán v registru plátců daně z přidané hodnoty jako nespolehlivý plátcem, má Objednatel právo uhradit za Poskytovatele DPH z tohoto zdanitelného plnění, aniž by byl vyzván jako ručitel správcem daně Poskytovatele, postupem v souladu s § 109a ZDPH. Pokud Objednatel uhradí částku ve výši DPH na účet správce daně Poskytovatele a zbývající částku sjednané ceny (tj. relevantní část bez DPH) Poskytovateli, považuje se jeho závazek sjednanou cenu za splněný. Dnem úhrady se rozumí den odepsání poslední příslušné částky z bankovního účtu Objednatele.

VI. ODPOVĚDNOST ZA VADY

- VI.1** Poskytovatel poskytuje Objednateli záruku za jakost servisních úkonů, oprav a jejich výsledků, jestliže to jejich povaha připouští, a to po dobu **6 měsíců**.

- VI.2** Poskytovatel je povinen dodat náhradní díly zcela nové, v plně funkčním stavu, v jakosti a technickém provedení odpovídajícímu platným právním předpisům, harmonizovanými českými technickými normami a ostatními ČSN, které se vztahují k dodávaným náhradním dílům nebo příslušnému Zařízení, a to zejména požadavkům zákona č. 22/1997 Sb., o technických požadavcích na výrobky, ve znění pozdějších předpisů, a souvisejících předpisů, v platném znění.

- VI.3** Poskytovatel se zavazuje, že každý náhradní díl dodaný dle této smlouvy včetně veškerých jeho komponent bude po dobu uvedenou v předaném záručním listu, nejméně však po dobu **24 měsíců** ode dne převzetí Objednatel podle této smlouvy (dále jen „**Záruční doba**“), způsobilý pro použití k obvyklému účelu a že si nejméně po tuto dobu zachová své vlastnosti v souladu s touto smlouvou a Zadávací dokumentací. Poskytovatel tedy poskytuje Objednateli záruku za jakost každého dodaného náhradního dílu v délce uvedené v předaném záručním listu, nejméně však po celou Záruční dobu.

- VI.4** Objednatel je vedle práv z vadného plnění a práv vyplývajících ze sjednané nebo poskytnuté záruky za jakost oprávněn uplatňovat i jakékoliv jiné nároky související s dodáním vadného plnění nebo s vadným poskytnutím servisního úkonu (např. nárok na náhradu újmy).
- VI.5** Objednatel je oprávněn vedle nároků z vad poskytnutých služeb a dodaných náhradních dílů uplatňovat i jakékoliv jiné nároky související s poskytnutými službami nebo dodanými náhradními díly (např. nárok na náhradu škody). Poskytovatel neodpovídá za škodu, která vznikla v důsledku zanedbání povinnosti Objednatele stanovené touto smlouvou.

VII. OSTATNÍ UJEDNÁNÍ

- VII.1** Poskytovatel prohlašuje, že si je vědom povinností vyplývajících zejména ze zákona č. 340/2015 Sb., zákon o registru smluv, ve znění pozdějších předpisů (dále jen „**zákon o registru smluv**“), a souhlasí se zveřejněním veškerých informací týkajících se závazkového vztahu vzniklého mezi Poskytovatelem a Objednatelem z této smlouvy, zejména se zveřejněním vlastního textu této smlouvy. Zveřejnění v registru smluv provede Objednatel.
- VII.2** Tato smlouva nabývá účinnosti dnem jejího uveřejnění v registru smluv podle zákona o registru smluv a uzavírá se **na dobu 6 let od nabytí účinnosti**.

VIII. MLČENLIVOST

- VIII.1** Strany této smlouvy jsou si vědomy toho, že v rámci plnění závazků z této smlouvy:
- a) si mohou vzájemně vědomě nebo opomenutím poskytnout informace, které budou poskytující stranou považovány za důvěrné (dále jen „**Důvěrné informace**“);
 - b) mohou jejich zaměstnanci a osoby v obdobném postavení, zejména osoby jednající z jejich pověření, získat vědomou činností druhé strany nebo i jejím opomenutím přístup k Důvěrným informacím druhé strany.
- VIII.2** Za Důvěrné informace se vždy považují:
- a) veškeré osobní údaje, jejichž správcem nebo zpracovatelem je Objednatel (dále jen „**Osobní údaje**“);
 - b) informace, které jako důvěrné smluvní strana výslovně označí;
 - c) veškeré informace související se zabezpečením Důvěrných informací;
 - d) veškeré informace související s provozem a zabezpečením zdravotnických prostředků, Zařízení, přístrojů, počítačových programů a dalších systémů Objednatele zpracovávajících Důvěrné informace; a
 - e) veškeré informace související s provozem a zabezpečením počítačových sítí a informační a komunikační infrastruktury Objednatele.
- VIII.3** Strana této smlouvy, která přijala Důvěrné informace nebo které byly Důvěrné informace z jakéhokoli důvodu zpřístupněny, je povinna s odbornou péčí zachovávat jejich důvěrnost a k ochraně jejich důvěrnosti vyvíjet alespoň takové úsilí, jako by se jednalo o její vlastní důvěrné informace.
- VIII.4** Smluvní strany se zavazují, že žádná z nich Důvěrné informace nepřístupní třetí osobě, nezveřejní ani je neužije v rozporu s účelem této smlouvy, a to ani pro svůj vlastní prospěch. Za třetí osoby podle věty první se nepovažují zaměstnanci Objednatele. Za třetí osoby podle věty první se nepovažují ani osoby, které jsou Poskytovatelem pověřeny k poskytování plnění dle této smlouvy. Poskytovatel je však povinen tyto osoby

zavázat k mlčenlivosti, zajišťování bezpečnosti informací a ochraně osobních údajů ve stejném rozsahu a za stejných podmínek, jako je k tomu sám zavázán podle této smlouvy. Poskytovatel je na písemnou výzvu Objednatele povinen Objednateli písemně prokázat existenci právního vztahu se třetí osobou splňujícího podmínky věty předchozí, a to do 10 pracovních dnů od doručení takové písemné výzvy.

VIII.5 Strany této smlouvy se zavazují ve vztahu k této smlouvě poučit veškeré osoby, které se na jejich straně podílejí nebo budou podílet na plnění této smlouvy, o povinnosti zachovávat mlčenlivost a chránit Důvěrné informace podle této dohody a právních předpisů.

VIII.6 Žádným ustanovením této smlouvy nejsou dotčeny povinnosti Objednatele vyplývající z právních předpisů, zejména ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a ze zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů.

IX. OCHRANA OSOBNÍCH ÚDAJŮ A BEZPEČNOST INFORMACÍ

IX.1 Poskytovatel se v souvislosti s povinnostmi Objednatele, které vyplývají z nařízení Evropského parlamentu a Rady (EU) ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), včetně adaptačních právních předpisů tohoto nařízení (dále souhrnně jen „**GDPR**“), zavazuje zpracovávat Osobní údaje výhradně na základě pokynů Objednatele a výhradně za účelem plnění povinností vyplývajících z této smlouvy.

IX.2 V případě události s dopadem na bezpečnost Zařízení, bezpečnost Osobních údajů nebo bezpečnost informací v Zařízení je Poskytovatel povinen předat Objednateli bez zbytečného odkladu, nejpozději však do 12 hodin od okamžiku, kdy Poskytovatel takovou událost při poskytování plnění dle této smlouvy měl nebo mohl zjistit, veškeré Poskytovateli dostupné informace o takové bezpečnostní události.

IX.3 Poskytovatel je povinen při poskytování plnění podle této smlouvy dodržovat zásady bezpečnosti informací a dat včetně osobních údajů (dále v tomto odstavci jen „**bezpečnost informací**“), jakož i zásady ochrany osobních údajů stanovených GDPR, přičemž bezpečností informací se rozumí zajišťování důvěrnosti, integrity a dostupnosti informací, které jsou uchovávány, vytvářeny nebo zpracovávány v Zařízení.

IX.4 Poskytovatel je povinen poskytovat Objednateli v souvislosti s poskytováním plnění dle této smlouvy součinnost k zavádění, provádění, revidování a aktualizaci technických a organizačních opatření týkajících se Zařízení a stanovených Objednatелеm za účelem souladu zpracovávání osobních údajů s GDPR. Jestliže vznikne v souvislosti s povinnostmi podle tohoto odstavce potřeba uzavřít dodatek k této smlouvě nebo zvláštní smlouvu, zavazuje se Poskytovatel poskytnout Objednateli veškerou součinnost nezbytnou k formulaci obsahu takového dodatku, resp. smlouvy, a k uzavření takového dodatku, resp. smlouvy v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění (dále jen „**ZZVZ**“), a dalšími právními předpisy.

IX.5 Kyberbezpečnost

Objednatel informuje Poskytovatele, že je osobou povinnou a provozuje informační systém základní služby podle zákona 181/2014 Sb., o kybernetické bezpečnosti a vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. Poskytovatel je povinen respektovat bezpečnostní opatření a relevantní požadavky na kybernetickou bezpečnost uvedené v dokumentu "Pravidla minimální kybernetické bezpečnosti pro dodavatele" (dále jen (Pravidla), který tvoří Přílohu č. 1 této smlouvy. Podpisem této smlouvy

Poskytovatel stvrzuje, že se s výše uvedenými Pravidly seznámil a je povinen je dodržovat.

X. SANKCE A ODSTOUPENÍ OD SMLOUVY

- X.1** V případě prodlení Poskytovatele s provedením servisních úkonů v termínech dle čl. II. této smlouvy je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši 1000,- Kč (slovy jeden tisíc korun českých), a za každý takový případ a za každý započatý kalendářní den prodlení.
- X.2** V případě, že Poskytovatel bude zpracovávat Osobní údaje v rozporu s touto smlouvou, je povinen zaplatit Objednateli smluvní pokutu ve výši 50 000 Kč (slovy: padesát tisíc korun českých) za každé takové porušení povinnosti.
- X.3** V případě prodlení Objednatele s úhradou faktur, je Poskytovatel oprávněn účtovat Objednateli úrok z prodlení ve výši stanovené dle občanského zákoníku.
- X.4** Uplatněná či již uhrazená smluvní pokuta nemá vliv na uplatnění nároku Objednatele na náhradu škody, kterou lze vymáhat samostatně vedle smluvní pokuty v celém rozsahu, tj. částka smluvní pokuty se do výše náhrady škody nezapočítává. Zaplacením smluvní pokuty není dotčena povinnost Poskytovatele splnit závazky vyplývající z této smlouvy.

XI. ZÁVĚREČNÁ UJEDNÁNÍ

- XI.1** Jakékoliv změny či doplňky této smlouvy lze činit pouze formou písemných číslovaných dodatků podepsaných oběma smluvními stranami; odstoupení od smlouvy lze provést pouze písemnou formou.
- XI.2** Tato smlouva je vyhotovena ve dvou (2) stejnopisech, s platností originálu, z nichž každá smluvní strana obdrží po jednom, bude-li smlouva uzavřena v listinné podobě. V případě, že je smlouva vyhotovena v elektronické podobě, jedná se o jedno vyhotovení s elektronickými podpisy obou účastníků smlouvy v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.
- XI.3** Nedílnou součástí této smlouvy je:
Příloha č. 1: Pravidla minimální kybernetické bezpečnosti pro dodavatele

V Uherském Hradišti dne

V Praze dne

.....
Uherskohradišťská nemocnice a.s.

MUDr. Petr Sládek
předseda představenstva

.....
Siemens Healthcare, s.r.o.

Mgr. Michal Čech a Ing. Karel Kopejtko
jednatelé společnosti

PRAVIDLA MINIMÁLNÍ KYBERNETICKÉ BEZPEČNOSTI PRO DODAVATELE

Uherskohradišťská nemocnice a.s.

Obsah

1	Úvodní ustanovení.....	3
1.1	Cíle dokumentu	3
2	Obecné povinnosti.....	3
3	Bezpečnost HW, SW a komunikace.....	4
3.1	Pracovní stanice, notebooky	4
3.2	Využívání internetu	4
4	KB systémů IT.....	5
4.1	Používání hesel.....	5
4.2	Monitorování používání a přístupu k systému	5
4.3	Řízení přístupu k informačnímu systému.....	6
5	Bezpečnost dat.....	6
5.1	Data vstupující do IS UHN	6
5.2	Data předávaná smluvním partnerům.....	7
6	KB dodávek a služeb.....	7
6.1	Vývoj software smluvními partnery	7
6.2	Dodávka software.....	8
7	Závěrečná ustanovení	8

1 Úvodní ustanovení

1. **Pravidla minimální kybernetické bezpečnosti pro dodavatele** Uherskohradištské nemocnice a.s. (dále též UHN) tvoří soubor závazných pravidel a postupů vymezujících způsob a požadovanou úroveň kybernetické bezpečnosti, vymezení aktiv (aktivum je cokoliv, co má hodnotu pro organizaci) a způsob jejich ochrany, týkající se firem a organizací se smluvním vztahem k UHN.
2. Dodržování pravidel uvedených v tomto dokumentu je povinné pro všechny smluvní partnery UHN, kterých se dotýká problematika kybernetické bezpečnosti.
3. Používané i nově zaváděné informační systémy v rámci UHN musí být upraveny, vyvíjeny a vybírány a spravovány tak, aby splňovaly zásady kybernetické bezpečnosti podle tohoto dokumentu.

1.1 Cíle dokumentu

1. Kybernetická bezpečnost (dále také „**KB**“) je ochrana elektronických informací, systémů a služeb proti živelním událostem, lidským omylům a úmyslné manipulaci s cílem snížit pravděpodobnost a dopad bezpečnostních incidentů na minimum.
2. Cílem Pravidel **minimální bezpečnosti pro dodavatele** s UHN je obecně:
 - a) specifikovat jasné zásady KB pro dodavatele UHN
 - b) zabránit neautorizovanému přístupu k informacím UHN,
 - c) umožnit provádění kontroly přístupu k informacím,
 - d) zajistit dostupnost informací pro oprávněné uživatele i procesy,
 - e) zabránit neautorizované modifikaci či zneužití dat nebo jiných aktiv a umožnit ověření původu informací,
 - f) definovat základní pravidla rozvoje a výběru nových používaných prostředků a technologií (vývoj zabezpečovacích prostředků, vlastnosti používaných aplikací a operačních systémů),

2 Obecné povinnosti

Mezi povinnosti smluvních partnerů patří zejména:

- a) používání informačních aktiv s UHN pouze v souladu s rozsahem přístupových oprávnění a pouze ke schváleným účelům,
- b) zajištění ochrany svých autentizačních údajů, (login, heslo, identifikační předmět)
- c) odpovědnost za každý přístup k informacím, provedený prostřednictvím jejich autentizačních údajů,
- d) respektování všech bezpečnostních opatření a procedur určených vlastníkem informací,
- e) nerozšiřování dat bez souhlasu vlastníka informací.

3 Bezpečnost HW, SW a komunikace

Smluvní partneři UHN musí chránit aktiva UHN, která používají ke své práci či výkonu pro UHN, a zabránit jejich poškození, zneužití nebo odcizení.

3.1 Pracovní stanice, notebooky

Při práci na koncových uživatelských pracovištích UHN musí být splněny nejméně následující bezpečnostní zásady:

- a) použití počítače UHN je umožněno pouze oprávněné osobě,
- b) je zakázáno připojovat vlastní počítače do vnitřní sítě UHN bez vědomí manažera kybernetické bezpečnosti nebo vedoucího útvaru Informační a komunikační technologie,
- c) pracovní stanice nesmí být ponechány bez dozoru zapnuté a s přihlášeným uživatelem. Je třeba přinejmenším použít heslem chráněného spořiče obrazovky,
- d) počítač smluvního partnera, který má být připojen do vnitřní sítě UHN, musí mít instalován a spuštěn systém pro ochranu před škodlivými programy (antivirový program) v nejnovější verzi programu i virové databáze,
- e) smluvní partner je povinen chránit vybavení UHN, udržovat okolo sebe bezpečné pracovní prostředí,
- f) v případě ukončení práce se zařízením je smluvní partner povinen provést odhlášení od systému, aby se zamezilo zneužití jeho přístupových práv.

3.2 Využívání internetu

1. Systémy v UHN vztahující se k počítačové síti, internetu a intranetu, včetně počítačového vybavení, programů, operačních systémů, medií pro ukládání dat, schránek elektronické pošty UHN, možností prohlížení internetových stránek a zdrojů přístupných na datových úložištích jsou vlastnictvím UHN.
2. Zaměstnanci smluvních partnerů mají dovoleno používat internetové připojení do a z vnitřní sítě UHN pouze za účelem činnosti pro UHN. Způsob připojení do vnitřní sítě UHN a autentizace musí být předem dohodnut s manažerem kybernetické bezpečnosti, vedoucím útvaru Informační a komunikační technologie UHN, nebo jím pověřeným pracovníkem odboru IT. Obecně musí platit povinnost oznámit předem datum a čas přihlášení k vnitřnímu prostředí a následně ukončení práce ve vnitřním prostředí UHN.
Pozn: Do „vnitřní sítě nemocnice“ nespadá připojení přes volnou wifi, poskytovanou UHN pacientům.

4 KB systémů IT

U vyvíjených, dodávaných a spravovaných informačních systémů musí být zajištěno dodržení níže uvedených povinností.

4.1 Používání hesel

- a) Aplikace musí být vytvářeny tak, aby znemožnily přístup bez zadání hesla.
- b) Aplikace musí být schopná ověřovat uživatele v Microsoft AD. Používání lokálních účtů v aplikaci je možné jen po odsouhlasení manažerem KB nebo vedoucím odboru IT. U svých lokálních uživatelů musí aplikace dodržovat následující pravidla:
- c) Uživatel aplikace musí být nucen si heslo pravidelně měnit.
- d) Aplikace musí být vytvořena tak, aby byl počet neúspěšných pokusů o přihlášení omezen. Po třech neúspěšných pokusech o přihlášení musí být další zadávání dočasně ochromeno nebo spojení rozpojeno.
- e) Pokud je při přihlašování do aplikace některá část zadaných informací chybná, nesmí být uživateli poskytnuta informace, ve kterém z údajů je chyba.
- f) V případě, že je povolen přístup do aplikace, v níž určuje vstupní heslo administrátor, je povinností autora aplikace vynutit si změnu tohoto inicializačního hesla.

- g) Všichni uživatelé musí při své činnosti užívat jedinečný identifikátor (přihlašovací jméno) tak, aby bylo možné vysledovat odpovědnost jednotlivců za prováděné činnosti.
- h) Zaměstnanci dodavatele smí používat jedno přihlašovací jméno pro několik svých zaměstnanců, přičemž dodavatel odpovídá za veškeré úkony provedené v informačním systému UHN pod těmito identifikátory.

4.2 Monitorování používání a přístupu k systému

V informačních systémech musí být pořizovány auditní záznamy obsahující minimálně:

- a) identifikaci uživatele,
- b) datum a čas přihlášení a odhlášení,
- c) identifikaci místa, odkud se uživatel přihlašoval (pokud je to možné),
- d) záznamy o přístupu (o úspěšném i neúspěšném pokusu o přihlášení).

Auditní záznamy musí být pořizovány tak, aby bylo možné jejich automatické sledování a vyhodnocování.

4.3 Řízení přístupu k informačnímu systému

- a) Před umožněním přístupu musí být každý uživatel identifikován a autentizován.
- b) Informační systém by měl po určité době nečinnosti uživatele (doporučeno 15 minut) tohoto uživatele odhlásit.
- c) Po určitém množství neúspěšných autentizačních pokusů (doporučeno 3) se musí ukončit přihlašovací procedura.
- d) V případě neúspěšné autentizace nesmí systém poskytnout uživateli informaci o tom, která část autentizace je chybná.
- e) Pro každého uživatele systému musí být možno identifikovat, jaká má přístupová práva.
- f) Pro každý informační systém musí být možno vytvořit seznam uživatelů, kteří mají přístupová práva k tomuto prostředku s rozlišením druhu přístupových práv (čtení, úprava atd.)
- g) Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo skupině.

5 Bezpečnost dat

5.1 Data vstupující do IS UHN

Data vstupující do systémů UHN musí být kontrolována, aby byla zajištěna jejich správnost. V aplikacích se musí evidovat identifikátor uživatele nebo procesu, který změny nebo pořízení provedl.

Pro kontrolu dat je nezbytné aplikovat opatření:

- a) Vstupní kontrola (neplatné znaky, rozsah, přetečení, kompletnost, souvislost...),
- b) kontrola vnitřního zpracování dat,
- c) kontrola oprávněnosti běhu programů,
- d) kontrola integrity dat,
- e) kontrola obsahu generovaných dat.

Opatření musí zahrnovat i popis postupu při zjištění chyby.

Pokud UHN usoudí, že vytvářená aplikace by měla podporovat kryptografii, je nezbytné, aby byly podporovány mezinárodně uznávané standardy a dodrženy právní předpisy České republiky.

5.2 Data předávaná smluvním partnerům

Jedná se o chráněné informace předávané z UHN smluvnímu partnerovi na jakémkoliv nosiči, zejména jakékoliv listiny, interní dokumenty UHN, CD-ROM, diskety, pevné disky počítačů a jiné nebo zasílané e-mailem. Smluvní partner musí nakládat s předávanými daty dle tohoto dokumentu.

- a) Předávání dat musí probíhat bezpečným způsobem.
- b) Uchovávání a případné zpracování dat u smluvního partnera musí být prováděno tak, aby byla zajištěna jejich ochrana před neoprávněným přístupem a aby bylo znemožněno jejich zneužití.
- c) Smluvní partner je povinen zajistit bezpečnou likvidaci již nepotřebných dat, případně médií s daty. Pro likvidaci médií nesoucích neveřejné informace musí být zvolena metoda, která zaručuje, že takto zlikvidované informace není možno běžně dostupnými prostředky obnovit (skartovačka, SW skartovačka).

Smluvní partner není oprávněn sám stahovat jakákoli data z IS UHN; vytváření souborů musí provést oprávněný zaměstnanec UHN a teprve takto vytvořená data smí být (na smluvním základě) předána partnerovi.

6 KB dodávek a služeb

6.1 Vývoj software smluvními partnery

1. Vývoj software musí probíhat:

- a. na testovacím prostředí odděleném od prostředí produkčního,
- b. na testovacích datech, která nejsou převzata z provozní databáze. Pokud je nutno použít data z provozní databáze, je nutno je anonymizovat,
- c. tak, že migrace do provozního prostředí může být provedena až po akceptaci výsledků testů ve vývojovém prostředí a formalizovaném a doložitelném odsouhlasení.

2. Přístup dodavatele do IS UHN

Vzdálený přístup dodavatele může být povolen pouze za podmínek dohodnutých s vedoucím útvaru Informační a komunikační technologie nebo osobou, kterou pověří. O každém novém dodavateli, kterému se se zřizuje vzdálený přístup, bude informován manažer KB. Manažer KB má oprávnění vzdálené přístupy dodavatelů revidovat.

6.2 Dodávka software

1. U veškerého dodávaného programového vybavení musí být zřejmé, zda se jedná o volně šířený software nebo program podléhající licenční a registrační politice.