Bezpečnostní politika Nemocnice Jihlava – externí

Datum vydání: **1. 6. 2023**

Verze: **02**

Počet stran: **22**

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

Schválil: **MUDr. Lukáš Velev, MHA**
Ředitel
Nemocnice Jihlava, p. o

Obsah

1. Bezpečnostní cíle a principy

Bezpečnostní politika (dále BP) stanovená v tomto dokumentu je obecně platná pro všechny dodavatele, obchodní partnery, externí poskytovatele IT-služeb apod., Nemocnice Jihlava (dále jen Nemocnice), dále uváděné pod souhrnným označením „třetí strany“, kteří mají na základě vzájemných pracovně právních nebo jiných smluvních vztahů oprávnění přistupovat zevnitř nebo zvenčí k počítačové síti, IS[1] , prostředkům ICT[2] Nemocnice a zpracovávaným informacím v jakékoliv podobě a formě.

1.1 Cíle

Nemocnice si v zájmu zajištění bezpečnosti informací stanovila tzv. bezpečnostní cíle:

1. chránit informace v souladu s jejich hodnotou, citlivostí a určením,
2. podporovat vytváření bezpečného prostředí, procesů a způsobů zpracování informací vedoucích k zajištění bezpečnosti informací jak interně, tak vně Nemocnice,
3. poskytovat bezpečnou infrastrukturu, informační a komunikační technologie a prostředky zpracování informací obsahující potřebné bezpečnostní funkce,
4. vzdělávat zaměstnance a pracovníky Nemocnice, včetně externích subjektů, v kybernetické bezpečnosti a neustále zvyšovat jejich bezpečnostní povědomí,
5. efektivně řídit a zvládat mimořádné situace a bezpečnostní incidenty a minimalizovat negativní dopady na informace a provoz Nemocnice.

1.2 Principy

Nejdůležitějším úkolem v této oblasti je, aby informace a informační technologie, se kterými Nemocnice pracuje, byly vždy spolehlivé, správné, důvěryhodné a chráněné před hrozbami. To je také hlavním důvodem zavedení bezpečnostních opatření, která mají zajistit bezpečnostní principy:

1. důvěrnost, což znamená zajištění přístupu k informacím pouze autorizovaným uživatelům s potřebným oprávněním.
2. integritu, jež obnáší zajištění správnosti, úplnosti a neporušenosti informací a procesů.
3. dostupnost, tj. že oprávnění uživatelé mají přístup k informacím tehdy, kdy je potřebují, nebo jsou jimi požadovány.

1.3 Schvalování a účinnost externí bezpečnostní politiky

Revize externí bezpečnostní politiky probíhá minimálně 1x ročně a zodpovídá za ni garant tohoto dokumentu, tj. osoba zastávající roli Manažera kybernetické bezpečnosti. Změnu této politiky nebo některých jejích částí je možné provést:

- dodatkem po připomínkovém řízení s dotčenými útvary a bez nutnosti schvalování ředitelem (v případě menších změn), nebo
- vydáním nové verze celého dokumentu (v případě podstatných změn), jež podléhá schvalovacímu procesu.

Nový nebo změněný dokument je předkládán k projednání a připomínkovému řízení provoznímu a technickému řediteli. Po ukončení připomínkového řízení je Manažerem kybernetické bezpečnosti předložen ke schválení řediteli Nemocnice.
Datem účinnosti schválené nové verze dokumentu automaticky pozbývá předcházející verze platnosti.
Schválené aktuálně platné znění BP se stanoveným datem účinnosti poté Manažer kybernetické bezpečnosti postupuje k distribuci oprávněným zaměstnancům Nemocnice (garantům aktiv) a všem třetím stranám, jež jsou k dodržování této politiky smluvně vázány.

---

[1] Pojmem "*Informační systém*" (IS) myšlen systém informačních a komunikačních technologií používaný napříč organizací ke zpracování informací, včetně jeho konkrétních subsystémů.

[2] Pojmem "Informační a komunikační technologie" (ICT) je myšleno jakékoliv technické či technologické zařízení, výpočetní technika a ostatní vybavení zajišťující činnost informačního systému a elektronickou komunikaci.

1.4 Význam používaných pojmů

Administrátor	Zaměstnanec nebo pracovník externího poskytovatele služeb, který zajišťuje správu IS / KS.
Aktivum	Hmotný nebo nehmotný majetek, který má pro Nemocnici určitou hodnotu. Za aktiva jsou považovány např. informace (nebo jejich skupiny, databáze), HW-vybavení, SW-vybavení, fyzické objekty, ale i personální zdroje nebo poskytované služby.
Primární aktiva	Informace zpracovávané v IS i mimo něj, a služby poskytované nemocnicí prostřednictvím IS.
Podpůrná aktiva	Technická aktiva (technické a programové vybavení a komunikační prostředky), tj. např. systémová data, SW, HW a podpůrné služby, jako např. bezpečnostní služby, dodávky energie apod., a osoby podílející se na správě, provozu a rozvoji IS (vč. podpůrných procesů).
BP	V tomto dokumentu Bezpečnostní politika externí – určená třetím stranám.
Garant	Osoba (zpravidla ve vedoucí funkci), která je odpovědná za přidělené aktivum, a z toho titulu je oprávněna mj. např. stanovit hodnotu aktiva, určovat způsoby nakládání s aktivem a definovat požadavky na jeho ochranu. Synonymem garanta je vlastník.
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016 / 679
ICT	Informační a komunikační technologie.
Informace	Jakýkoliv údaj, který Nemocnice zpracovává v elektronické nebo fyzické (tištěné) a jiné podobě nejen prostřednictvím ICT.
IS	Informační systém(y), nebo také jen systém(y).
ISMS	Systém řízení bezpečnosti informací (z angl. Information Security Management System).
KS	Komunikační systém(y).
NDA	Dohoda o mlčenlivosti (z angl. Non Disclosure Agreement)
Nemocnice	Nemocnice Jihlava
OS	Operační systém
PIM/PAM	Privileged Identity Management a Privileged Access Management – jsou nástroje, které pomáhají s ochranou privilegovaných účtů a přístupem na kritické systémy infrastruktury. Jsou schopny zajistit jak řízený přístup, tak monitorování aktivity správců a rotaci hesel privilegovaných účtů včetně analytických funkcí.
PKI	Infrastruktura veřejných klíčů (z angl. Public Key Infrastructure)
Pracovník	Zaměstnanec externí právnické osoby nebo externí fyzická osoba v pracovně právním vztahu k nemocnici.
Správce IS / KS	Orgán nebo osoba, které určují účel zpracování informací a podmínky provozování informačního nebo komunikačního systému.
Třetí strana	Externí právnická nebo fyzická osoba, s níž Nemocnice uzavírá smluvní vztah např. k zajištění některých činností nebo přístupu k ICT / informacím.
Uživatel	Fyzická osoba, která je oprávněna přistupovat k ICT / informacím Nemocnice na základě přiděleného uživatelského účtu a přístupových oprávnění. Uživatelem může být zaměstnanec Nemocnice i pracovník třetí strany.
Zaměstnanec	Osoba v pracovně-právním vztahu k Nemocnici.

1.5 Související právní předpisy

Definice bezpečnostních standardů vychází mj. z právních předpisů, jimiž je Nemocnice vázána:

- Zákon č. 110 / 2019 Sb., o zpracování osobních údajů
- Nařízení Evropského parlamentu a Rady (EU) 2016 / 679 (tzv. Obecné nařízení nebo „GDPR“)
- Zákon č. 297 / 2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

- Zákon č. 121 / 2000 Sb., autorský zákon
- Zákon č. 499 / 2004 Sb., o archivnictví a spisové službě a o změně některých zákonů
- Zákon č. 418 / 2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim
- Zákon č. 90 / 2012 Sb., o obchodních korporacích
- Zákon č. 262 / 2006 Sb., zákoník práce

2. Minimální bezpečnostní požadavky na třetí strany

Nemocnice touto externí bezpečnostní politikou stanovuje minimální bezpečnostní požadavky, které musí dodržovat všechny tzv. třetí strany požadující přístup k ICT či informacím Nemocnice. Tyto požadavky představují povinnost zavedení a dodržování určitých opatření, která jsou rozdělena do dvou skupin:

3. Organizační opatření

Každá třetí strana, která požaduje přístup k ICT a informacím, musí splnit všechny relevantní níže uvedené minimální bezpečnostní požadavky Nemocnice týkající se oblasti organizačních opatření.

3.1 Požadované role a funkce

Nemocnice uplatňuje systém řízení bezpečnosti informací prostřednictvím ustanovených funkcí či rolí s přidělenými kompetencemi, pravomocemi a odpovědnostmi. Z toho důvodu musí být určeny a personálně obsazeny minimálně následující funkce / role:

- Nemocnice jako poskytovatel přístupu:
  - Manažer kybernetické bezpečnosti
  - Administrátor
- Subjekt třetí strany požadující přístup na základě smluvního vztahu:
  - Externí odpovědná osoba (kontakt podle smluvního ujednání)
  - Externí poskytovatel (garant) služby (servisní pracovník nebo dále také externí uživatel)

3.2 Požadovaná bezpečnostní dokumentace

K řízení bezpečnosti informací a zajištění kontinuity činnosti používá Nemocnice bezpečnostní dokumentaci. Z toho důvodu musí být vytvořena, příp. dle smluvních ujednání dodána nebo alespoň k dispozici také relevantní provozně-bezpečnostní dokumentace třetích stran týkající se jimi dodávaných nebo spravovaných IS nebo ISZS.
Požadovaný rozsah a obsah jednotlivých dokumentů se stanovuje na základě smluvních ujednání. Splnění požadavků na bezpečnost informací v provozně-bezpečnostní dokumentaci může být prokázáno také doložením platného certifikátu systému řízení bezpečnosti informací (např. dle ISO 27001), který zahrnuje oblast dodávky či správy IS nebo ISZS třetí stranou.

3.3 Požadavky ve smluvních vztazích se třetími stranami

Nemocnice požaduje, aby byl přístup třetích stran (pokud se jedná o vzdálený přístup k ICT a informacím Nemocnice, časově omezený zásah nebo jinou obdobnou činnost externích servisních pracovníků třetích stran) upraven:

- vždy smluvně,
- v souladu s touto BP,
- tak, aby byla zajištěna bezpečnost ICT a informací uvnitř i vně Nemocnice.

Požadavky na ochranu ICT a informací podle této BP (tj. primárním nebo podpůrným aktivům) musí být zakotveny ve smluvních ujednáních s třetími stranami:

- ještě předtím, než bude povolen a aktivován schválený přístup,
- pouze v rozsahu nezbytně nutném pro výkon smluvních závazků,
- jejichž součástí musí být ustanovení o povinné mlčenlivosti (tzv. NDA [3]), případně i požadavek adresnosti, tzn. jmenovité uvedení fyzických osob, kterým má být přidělen přístup a oprávnění.

3.3.1 Kategorie dodavatelů

Nemocnice stanovuje minimální bezpečnostní požadavky na třetí strany v závislosti na zařazení dodavatele do některé z níže uvedených kategorií:

A. **Standardní dodavatelé bez přístupu** – tj. zpravidla bez přístupu k primárním aktivům (informacím) Nemocnice, pouze s omezeným přístupem k podpůrným aktivům (ICT) v rámci dodávky:
   - standardní NDA Nemocnice nebo dodavatele (po vzájemné dohodě).

B. **Standardní dodavatelé s přístupem k ICT** – tj. zpravidla s omezeným přístupem k podpůrným aktivům (ICT) v rámci dodávky nebo poskytování IT-služeb, a s pouze nahodilým, dočasným nebo jen jednorázovým přístupem k primárním aktivům (informacím či službám) Nemocnice:
   - standardní NDA Nemocnice,
   - SLA,
   - smluvní ujednání,

C. **Dodavatelé s přístupem k informacím a ICT** – zpravidla „významní dodavatelé“ a provozovatelé VIS (viz kapitola 3.3.3) s přístupem k primárním a podpůrným aktivům (ICT anebo informacím) Nemocnice v rámci dodávky anebo poskytování IT-služeb:
   - NDA Nemocnice (viz kapitola 3.3.2),
   - SLA,
   - smluvní ujednání dle přílohy č. 7 k VoKB – viz příloha v kapitole č. 5.2.

3.3.2 Dohoda o mlčenlivosti (NDA)

S dodavateli IT služeb, kteří pro výkon smluvních povinností potřebují přístup k aktivům Nemocnice, musí být povinně ještě před povolením přístupu uzavřena písemná Dohoda o mlčenlivosti (NDA)[4] , obsahující zejména:

---

[3] NDA = angl. zkratka „non disclosure argumenty“ - ujednání o mlčenlivosti

[4] NDA je dohoda o mlčenlivosti uzavíraná mezi nemocnicí a dodavatelem IT služeb, ve které se následně omezí využití takového přístupu dodavatelem mimo sjednaný účel spolupráce a omezí předání přístupů případné třetí straně.

- identifikaci správce nebo provozovatele,
- identifikaci informačního a komunikačního systému,
- identifikaci významného dodavatele,
- vyrozumění o skutečnosti, že dodavatel je pro správce významným dodavatelem, a popřípadě také o tom, že významný dodavatel je zároveň provozovatelem,
- obsah pravidel, tj. minimálně:
    - Politika přístupových práv,
    - Servisní smlouva stanovující úroveň služeb (SLA),
    - Monitoring,
    - Ochrana duševního vlastnictví,
    - Způsob předání / výmazu informací při ukončení smlouvy.

Seznam dodavatelů, se kterými byla podepsána „NDA“, případně mají povolen přístup k primárním či podpůrným aktivům Nemocnice, eviduje vždy garant aktiva (případně po dohodě s garantem Manažer kybernetické bezpečnosti).
Existence, trvání a plnění povinností vyplývajících ze smluv pro dodavatele (vč. NDA, SLA) musí být pravidelně (min. 1x ročně) kontrolována. Za kontrolu odpovídá vždy příslušný garant, který o kontrole vede záznam ve své evidenci.

3.3.3 Významní dodavatelé

Smluvní ujednání se třetími stranami, které byly zařazeny na seznam „Významných dodavatelů“[5] Nemocnice a informovány o tom, že se staly „Významným dodavatelem“ a provozovatelem ISZIS, musí obsahovat minimálně následující body (v souladu s přílohou č. 7 k VoKB, viz příloha v kapitole č. 5.2):

- definice „chráněné informace“,
- vzájemná odpovědnost,
- doba trvání smlouvy,
- vymezení pojmů,
- sankce v případě porušení,
- zmínění akcí, které budou následovat v případě porušení smlouvy,
- úprava pravidel o předávání informací třetím stranám,

případně také (dle relevance):

- instrukce o nakládání s osobními údaji,
- opatření pro nakládání s majetkem,
- školení osob, které budou nakládat s chráněnými informacemi,
- revize a zánik smlouvy.

3.4 Požadovaná ochrana klasifikovaných informací

Informace Nemocnice mají přiděleny stupně ochrany podle jejich citlivosti. Jednotlivé stupně klasifikace informací mají současně stanoveno povolené zacházení s nimi, a to jak v elektronické, tak v písemné (tištěné) a jiné podobě, tj.:

- v průběhu jejich vstupu do IS, ukládání, přepravy či přenosu, např. e-mailem, poštou, internetem,
- ve všech formách výstupu, tisku, kopírování, ústního sdělení, zálohování, archivace a likvidace.

Pokud třetí strany v rámci smluvně dohodnuté činnosti získají přístup k informacím střední a vyšší úrovně klasifikace, musí dodržovat minimální požadavky na ochranu a způsob zacházení s nimi podle klasifikace aktiv, která tvoří samostatnou přílohu k této BP – Klasifikace aktiv.

3.5 Požadovaná personální opatření

Nemocnice uplatňuje bezpečnostní požadavky na zajištění personálních procesů týkající se externích subjektů, tj. třetích stran, včetně jejich případných subdodavatelů.
Pokud třetí strany vyžadují v rámci smluvních vztahů k zajištění své činnosti přidělení přístupu k ICT a

[5] Významným dodavatelem je takový dodavatel, který je zároveň provozovatelem informačního nebo komunikačního systému, nebo každý, kdo s nemocnicí vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému, viz metodický dokument MZ ČR Politika řízení dodavatelů a metodický dokument NÚKIBu Provozovatel informačního nebo komunikačního systému podle § 2 písm. g) ZoKB.

informacím Nemocnice, musí v zájmu bezpečnosti dodržovat procesy a postupy stanovené touto politikou.

- Uzavření smluvního vztahu s třetí stranou schvaluje ředitel.
- Přidělení přístupu třetí strany k ICT a informacím Nemocnice schvaluje Manažer kybernetické bezpečnosti, nebo Náměstek pro informatiku a kybernetickou bezpečnost.

Teprve po schválení ředitelem (v případě smluvních ujednání se třetí stranou) je administrátor systému oprávněn požádat o vzdálený přístup třetí strany. Žádost musí schválit Manažer kybernetické bezpečnosti, nebo Náměstek pro informatiku a kybernetickou bezpečnost. Požadavek (Žádost o přístup) je následně zpracován automatizovaně (v případě RDP), nebo předáván administrátorovi Nemocnice, který:

- zřizuje, mění nebo ruší uživatelský účet externího uživatele,
- přiděluje či odebírá příslušná oprávnění externího uživatele.

3.6 Požadavky na žádost o přístup

Formální požadavek na přidělení, změnu či odebrání uživatelských účtů a přístupů k primárním a podpůrným aktivům (ICT a informacím) Nemocnice musí obsahovat minimálně:

- kontakt na žadatele,
- zdůvodnění požadavku na přístup (může být uvedeno např. číslo smlouvy)
- rozsah přístupu (tj. ke kterým systémům / aplikacím / informacím může žadatel přistupovat),
- název firmy,
- oprávněnou osobu (konkrétní pracovník třetí strany s požadovaným přístupem),
- email a telefonní číslo oprávněné osoby (konkrétní pracovník třetí strany s požadovaným přístupem)

Žádost dále obsahuje následující parametry:

- stav schválení žádosti o přístup,
- stav žádosti (čekající na schválení, probíhá vytváření přístupu, proces selhal, zamítnuta, prodlužování expirace, přístup vytvořen),
- období přístupu (defaultně j nastaveno na 1 rok od vytvoření, žadatel je povinen přístup deaktivovat prostřednictvím editace žádosti, nejpozději do termínu vypršení smlouvy),
- OTP – stav nastavení MFA (aktualizuje se automatizovaně),
- datum posledního přístupu (aktualizuje se automatizovaně),
- IP adresa posledního přístupu (aktualizuje se automatizovaně),
- město posledního přístupu (aktualizuje se automatizovaně).

3.7 Požadavky na odpovědnost třetích stran

Spolu s převzetím přístupu přiděleného třetí straně na základě schválené žádosti musí třetí strana zajistit:

- prokazatelné převzetí odpovědnosti oprávněných osob,
- prokazatelný závazek mlčenlivosti (např. ve smluvních ujednáních nebo oproti podpisu na schválené žádosti o přístup),
- minimální úroveň bezpečnostního povědomí všech fyzických osob třetí strany s přístupem k ICT a informacím Nemocnice, např. prokazatelným seznámením nebo zaškolením pracovníků třetích stran s touto BP,

a to např. ve smluvních ujednáních.

3.8 Požadavky na zrušení přístupu

Pro případ ukončení smluvního vztahu se třetí stranou musí být:

- definován formální požadavek na zrušení všech přidělených uživatelských účtů a přístupů k ICT a informacím Nemocnice:
  - kde budou specifikovány konkrétní kroky nutné k odebrání přístupu či oprávnění, k navrácení nebo bezpečné likvidaci dat nacházejících se u třetí strany,
- definovány činnosti, které musí třetí strana dodržet při vzájemném vypořádání:
  - tak, aby nedošlo k narušení kontinuity činnosti Nemocnice,

a to např. ve smluvních ujednáních nebo v dodatku k nim.

3.9 Požadavky na detekci a hlášení bezpečnostních událostí

Třetí strany musí být schopni, v závislosti na zařazení do kategorie dodavatelů „B“ nebo „C“ (viz kapitola 3.3.1), detekovat kybernetické bezpečnostní události a identifikovat kybernetické bezpečnostní incidenty. Všichni pracovníci třetích stran s přístupem k ICT a informacím Nemocnice jsou povinni (v rámci svých pracovních povinností nebo podle smluvních ujednání) dohodnutým způsobem hlásit zjištěné závady, poruchy, incidenty, podezřelé aktivity, případně odhalené slabiny odpovědné osobě třetí strany, potažmo administrátorovi Nemocnice nebo Manažerovi kybernetické bezpečnosti Nemocnice.

4. Technická opatření

4.1 Technické řešení vzdáleného přístupu

Vzdálený přístup je 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.

4.2 Požadavky na bezpečnost objektů

Nemocnice stanovila fyzické bezpečnostní okruhy týkající se ochrany objektů, v nichž jsou umístěna primární či podpůrná aktiva (prostředky ICT nebo informace), a ve kterých musí být v souladu s typem objektu dodržovány minimální požadavky a prvky fyzického zabezpečení. Tyto zabezpečené oblasti tvoří samostatnou přílohu k této BP.

- V případě fyzického přístupu pracovníků třetích stran do objektů Nemocnice musí tito pracovníci dodržovat požadavky na objektovou bezpečnost ve fyzických zabezpečených oblastech, kam mají v rámci plnění smluvních závazků a schválené žádosti oprávněn fyzický vstup.
- V případě ICT a informací umístěných, spravovaných nebo poskytovaných mimo objekty Nemocnice, tzn. u třetích stran, musí tyto strany zajistit adekvátní naplnění požadavků na prvky objektové bezpečnosti tak, aby nemohlo dojít k neoprávněnému fyzickému přístupu k ICT a informacím Nemocnice.

4.3 Požadavky na bezpečnost zařízení

Zařízení a vybavení, které slouží k zajištění provozu podpůrných aktiv (ICT nebo podpůrných služeb), musí být chráněno před fyzickými hrozbami, jako jsou přírodní události (oheň, voda, mráz, vítr) nebo působení lidského činitele, jejichž výsledkem může být havárie, porucha, poškození, zničení, krádež apod. Mezi zařízení a vybavení, která musí být chráněna v objektech Nemocnice i třetích stran, a na kterých je závislá provozuschopnost ICT, patří:

- výpočetní technika, switch / router, přístupové zařízení (AP), kabeláž, tiskárna, skener, kopírka,
- zdroje energie, jističe, UPS, agregáty,
- klimatizace, dodávky tepla, vody.

Všichni pověření, resp. oprávnění pracovníci třetích stran jsou povinni zabezpečit fyzický přístup k zařízení a vybavení ve všech lokalitách, kde jsou umístěny ICT, IS nebo jejich komponenty (v elektronické i tištěné podobě), před výše uvedenými fyzickými hrozbami jak v mimopracovní době, tak i v případě krátkodobého opuštění pracoviště, zejména těmito opatřeními:

- dodržování zásady „čistého stolu“, tzn. bezpečné ukládání dokumentů v listinné podobě a nosičů dat a médií podle citlivosti obsažených informací (v souladu s klasifikací informací) - do uzamykatelných schránek (zásuvka, skříň, trezor),
- důsledné zamykání kanceláře,
- fyzická ochrana klíčů, vstupních / čipových karet apod.,
- zákaz kouření a práce s nebezpečnými látkami na pracovišti.

Povinnosti fyzické ochrany (tj. zvýšená opatrnost a používání prostředků fyzické bezpečnosti) se vztahují

i na mobilní zařízení, jako jsou např. přenosné počítače, notebooky, tablety, nosiče dat a média, pokud fyzicky opouštějí zabezpečené oblasti Nemocnice a jsou používány v objektech nechráněných bezpečnostními perimetry[6] .

4.4 Požadavky na kontrolu fyzického přístupu

Fyzický vstup návštěvníků a externích pracovníků třetích stran do zabezpečených oblastí objektů Nemocnice musí být kontrolován. K prostředkům ICT, které jsou umístěny v zabezpečených oblastech Nemocnice nebo třetích stran, je fyzický přístup vyhrazen pouze povolaným a oprávněným osobám, kterými mohou být:

- zaměstnanci Nemocnice na základě jim přidělených oprávnění, nebo
- pracovníci třetích stran na základě smluvních ujednání.

Všem ostatním osobám je fyzický přístup a používání ICT Nemocnice zakázáno.

4.5 Požadavky na řízení přístupu k informacím

Základními požadavky při řízení tzv. „logického“ přístupu, tedy přístupu externího uživatele na základě přihlášení uživatelským účtem s přístupovým oprávněním k informacím zpracovávaným v ICT, jsou:

- primární zákaz nebo alespoň maximální omezení všech práv. Postupné rozšiřování a přidělování práv je možné pouze se souhlasem garanta informací, potažmo Manažera kybernetické bezpečnosti Nemocnice, který posuzuje oprávněnost přístupu, a na základě písemného požadavku externí odpovědné osoby, která posuzuje potřebnost přístupu externího uživatele;
- každá organizace (třetí strana a její pracovníci) musí mít přidělen svůj vlastní (jmenovitý) externí uživatelský účet pro každou fyzickou osobu;
- zákaz sdílení jednoho administrátorského přístupu (účtu) více fyzickými osobami;
- každý pracovník třetí strany (externí uživatel) musí být odpovědný za ochranu jemu přidělených přihlašovacích údajů (jméno, heslo, PIN, další autentizační údaje).

4.5.1 Standardy pro přidělování přístupu

Každému externímu uživateli je na základě schváleného požadavku přidělován přístup, jehož rozsah určuje garant aktiva. Nadstandardní rozšíření přístupu a výjimky jsou řešeny individuálně:

- podle specifických potřeb určovaných garantem aktiv,
- v souladu s interní klasifikací informací.

Pracovníci třetích stran s přidělenou možností hlásit se k IS zvenčí musí používat zabezpečený způsob přístupu a autentizace dle aktuálně používaných metod přístupu pro dodavatele.

4.5.2 Používání privilegovaného přístupu

Za privilegovaný přístup je považován takový přístup (např. administrátorský), který umožňuje uživateli spravovat systém, tzn. zasahovat do jeho konfigurace, provádět změny, vytvářet či rušit účty a přístupy dalším uživatelům apod. Privilegované (administrátorské a podobné) účty přidělené pracovníkům třetích stran je dovoleno používat pouze pro správu systémů, nikoliv k běžné činnosti těchto externích uživatelů. Jeden účet nesmí být sdílen více administrátory, pokud je to technicky / provozně možné. Pro třetí strany jsou uplatňovány následující požadavky:

- Přidělení privilegovaného (resp. administrátorského) přístupu k ICT Nemocnice třetí straně musí schválit Manažer kybernetické bezpečnosti, nebo Náměstek pro informatiku a kybernetickou bezpečnost.
- Uživatelé bez oprávnění administrace systému Nemocnice musí mít systémově odepřen přístup k těmto činnostem a nesmí jim být dovoleno svévolně vytvářet další účty a přístupy k operačnímu systému počítače, z nějž přistupují k ICT a informacím nemocnice.
- Na všech počítačích s přístupem k ICT a informacím Nemocnice je povolen výskyt pouze administrátorem předem definovaných účtů a musí být povinně zrušeny / zakázány všechny obecné účty vytvářené např. při instalaci OS s přednastaveným přístupem (typu „guest“, „anonymous“ apod.).

[6] Perimetr = hraniční prvek objektu, jako např. budova / zdi, uzamykatelné dveře, schránka / trezor apod.

- Každý externí uživatel se musí korektně přihlašovat k danému systému svým jedinečným identifikátorem (jménem a heslem) příp. jiným povoleným způsobem identifikace a autentizace, tj. ověření uživatele vůči systému, využití schválených autentizačních prostředků, HW tokenů, čipových karet, digitálních certifikátů apod.
- Pokud aplikace využívají vlastní omezení přístupu k informacím zpracovávaným jejich prostřednictvím, pak tato omezení nesmějí být v rozporu se stanovenou BP přístupových práv a úrovní přístupu (zejména ke klasifikovaným informacím) pro konkrétní externí uživatele či jimi zastávané funkce.

4.6 Požadavky na hesla

Pro oprávněný přístup třetích stran musí být používána přístupová hesla, která splňují stanovená kvalitativní kritéria:

- vygenerované prvotní heslo musí být uživateli předáváno bezpečným způsobem,
- přidělené heslo k uživatelskému účtu musí být při prvním přihlášení uživatelem změněno,
- musí být uplatňována více faktorová autentizace, nebo:
    - heslo musí být dlouhé minimálně:
        - 12 znaků (pro běžné uživatele)
        - 17 znaků (pro privilegované účty)
- heslo musí mít nastaveno datum expirace,
- heslo musí být změněno každých 18 měsíců,
- opakované použití stejného hesla musí být omezeno, tj. že systém si musí pamatovat nejméně 12 hesel v historii,
- systém musí limitovat počet neúspěšných pokusů o přihlášení, tj. zablokovat přístup po 5 pokusech,
- heslo nesmí být nikde ukládáno v čitelné (nechráněné) podobě, a to jak ve fyzické, tak v elektronické podobě,
- heslo může být změněno nejdříve za 30 minut po předchozí změně.

4.7 Požadavek čistého stolu a obrazovky

V případě fyzického opuštění pracoviště v Nemocnici nebo v místě, odkud se pracovník třetí strany přihlašuje k ICT Nemocnice, je povinností externího uživatele zabezpečit pracoviště i pracovní stanici před neoprávněným fyzickým i logickým přístupem jiných osob takovým způsobem, který je přiměřený délce nepřítomnosti, jako např.:

- odhlášení uživatele,
- uzamknutí stanice,
- aktivace spořiče obrazovky chráněného kvalitním heslem,
- bezpečné uložení nosičů dat a výtisků klasifikovaných informací,
- uzavření oken, uzamčení místnosti,
- aktivace zabezpečovacího systému / EZS apod.

Jedná-li se o nepřetržitý provoz, při němž se nelze odhlásit ze systému a stanice či konzola serveru musí zůstat v provozu např. i v nočních hodinách, je nezbytné zamezit přístupu k systému nepovolaným osobám jinými vhodnými opatřeními, která stanoví Manažer kybernetické bezpečnosti.
Všechny neaktivní stanice či terminály musí být po definovaném čase nečinnosti automaticky zablokovány.

4.8 Požadavky na ochranu mobilních prostředků a práci na dálku

Nemocnice uplatňuje politiku ochrany přístupu k mobilním prostředkům používaným vně (tzn. mimo chráněné prostředí počítačové sítě) Nemocnice, jako jsou např. notebooky, „chytré“ mobilní telefony, SD-karty a další zařízení či média fungující jako nosiče dat, kde mohou být potenciálně ohroženy klasifikované informace.
Používá-li pracovník třetí strany mobilní prostředky, v nichž se nacházejí chráněné informace Nemocnice klasifikované vyšší než „nízkou“ úrovní (veřejné informace), je povinen takové prostředky zabezpečit některým ze stanovených způsobů:

- ochrana zařízení (dle typu mobilního prostředku),
- ochrana přístupu k informacím v zařízení (dle typu např. PIN, gesto, biometrika, více faktorová autentizace),
- šifrování dat (šifrovací nástroj a použití kvalitního hesla viz kapitola 4.5),
- příp. fyzická ochrana mobilního prostředku (přenosná schránka chráněná zámkem s kódem).

Dostatečnost zabezpečení mobilních prostředků používaných k práci na dálku s ICT a informacemi v Nemocnici posuzuje, případně vhodné metody ochrany konkrétních mobilních prostředků stanovuje administrátor ve spolupráci s Manažerem kybernetické bezpečnosti.

4.9 Požadavky na IT procesy

Všechny důležité nebo kritické **IT-procesy** v rámci podpůrných aktiv (dále jen „**podpůrné IT-procesy**“) týkající se provozu, zpracování dat a služeb poskytovaných třetími stranami, **na kterých jsou závislá primární aktiva**, musí být definovány, popsány a spravovány podle potřeby tak, aby:

- bylo možno je zabezpečit,
- bylo možno zajistit zastupitelnost jednotlivých výkonných rolí.

4.9.1 Garant IT-procesu

Podpůrné IT-procesy mají přiřazeného garanta (vlastníka procesu), který je zodpovědný za jejich správné provádění. Administrátor je garantem podpůrných IT-procesů a odpovídá za jejich identifikaci, přidělení priorit a kontrolu výkonu smluvně dohodnutých IT-procesů a souvisejících činností pracovníků třetích stran.

Garant podpůrných IT-procesů odpovídá za jejich dokumentaci, popis postupů, jejich aktuálnost a evidenci. Garantem procesu může být stanoven i zástupce třetí strany, jedná-li se o zajištění podpůrných IT-služeb externím dodavatelem. V takovém případě může být zpracování dokumentovaných postupů smluvně vyžadováno po dodavateli takové služby.

Manažer kybernetické bezpečnosti je oprávněný zajišťovat nezávislou kontrolu podpůrných IT-procesů – revizi postupů třetí strany z hlediska dostatečnosti IT-procesů, aktuálnosti, schválených přístupů a ochrany dat odpovídající jejich klasifikaci.

4.9.2 Dokumentace podpůrných IT-procesů

Dokumentace podpůrných IT-procesů zajišťovaných třetí stranou musí obsahovat minimálně:

- garanta procesu;
- popis způsobu zpracování a nakládání s informacemi Nemocnice;
- požadavky na plánování kapacit, příp. závislost na jiných systémech;
- kontaktní osobu / místo pro hlášení a řešení technických či provozních potíží (např. ServiceDesk);
- zásady pro práci s klasifikovanými informacemi v rámci IT-procesů a jejich zabezpečení;
- postup obnovy IT-procesu po závadě, poruše, mimořádné události nebo havárii.

4.9.3 Hlášení incidentů podpůrných IT-procesů

Definování, popis a určení priority podpůrných IT-procesů slouží pro stanovení odpovídající reakce na pravděpodobné bezpečnostní incidenty v těchto procesech. Řízení incidentů obecně přísluší Manažerovi kybernetické bezpečnosti.

V případě zajišťování podpůrných IT-procesů třetí stranou musí být aplikovány následující kontrolní mechanismy vzájemné komunikace s odpovědnými osobami Nemocnice, zejména pro:

- hlášení závad a selhání podpůrných IT-procesů;
- hlášení bezpečnostních incidentů a zranitelných míst (slabin) systémů;
- kontrolu ztráty nebo porušení důvěrnosti informací v systémech spravovaných třetími stranami;
- pravidelné sledování a vyhodnocování auditních záznamů systémů spravovaných třetími stranami.

4.9.4 Zajištění zastupitelnosti

V případě podpůrných IT-procesů realizovaných třetí stranou je uplatňován požadavek na zachování kontinuity. Třetí strana musí zajistit zastupitelnost pracovníků v době jejich nepřítomnosti. Pro tyto případy musí být v dokumentaci třetí strany uvedena podrobná pravidla (např. pro ukládání, resp. obnovu hesel

a přístupových kódů pro mimořádné události, prokazatelné přidělení příslušných oprávnění zastupujícím pracovníkům, požadavky přesměrování komunikace apod.).

4.10 Požadavek na oddělení procesů vývoje od ostrého provozu

Vývoj programového vybavení je řešen dodavatelsky. Pokud dochází k implementaci SW-nástrojů či k úpravám systémů třetí stranou, musí být zajištěno, aby proces testování nového systému či SW nezasahoval do produkčního prostředí (do „ostrého provozu“), a to zejména v případě, kdy by mohl negativně ovlivnit provozuschopnost podpůrných IT-procesů nebo bezpečnost „ostrých dat“. Migrace do ostrého provozu musí respektovat stanovené bezpečnostní zásady a pravidla Nemocnice zajišťující, že nedojde k neplánovanému přerušení činnosti nebo kompromitaci dat.

4.10.1 Změnové řízení

Implementace významných změn (např. přechod na jiný systém, infrastruktury do cloudu, změna dodavatele systému nebo nový informační systém) v systému realizovaných třetí stranou podléhá formalizovanému procesu změnovému řízení, v jehož rámci jsou změny autorizovány odpovědnými osobami. Požadované změny musí být ještě před implementací technicky přezkoumány administrátorem a schváleny Manažerem kybernetické bezpečnosti.
Třetí strany jsou povinny u programového vybavení, OS a IS, jejichž správu a provoz zajišťují:

- omezit modifikace programových balíků (customizace ap.) na nezbytné minimum,
- kontrolovat opravné „balíčky“ před jejich implementací do ostrého provozu, s ohledem na ochranu před možnými hrozbami, skrytými kanály a trojskými koni,
- v případě vývoje nového SW externím dodavatelem je nutno zajistit příslušné bezpečnostní kontroly a smluvně ošetřit rizika.

4.11 Požadavky na ochranu před škodlivým SW

Informační systémy třetí strany, z nichž se v rámci oprávnění připojují pracovníci k systémům Nemocnice, musí být chráněny před škodlivými kódy pomocí vhodného SW. Antivirová ochrana obecně musí plnit jak detekční funkce, tak podle možností a potřeby i preventivní opatření k zabránění průniku nebo rozšíření škodlivého SW do systémů Nemocnice. Jsou uplatňovány následující minimální požadavky:

- všechny počítačové stanice, včetně mobilních zařízení, s přístupem k informacím Nemocnice jsou kontrolovány na přítomnost škodlivého kódu a musí mít povinně zapnutou rezidentní AV ochranu;
- na všech počítačových stanicích a mobilních zařízeních musí být zakázáno vypnout či omezit tuto ochranu uživatelem;
- pro všechny pracovníky třetích stran platí zákaz zasahovat do HW a SW konfigurace počítače, k němuž jim byl přidělen přístup, pokud to nevyžaduje plnění smluvních závazků;
- správnost, aktuálnost a účinnost nastavení AV ochrany musí být pravidelně kontrolována a ověřována;
- zveřejněné opravné balíky (záplaty) jsou po nezbytném ověření funkčnosti neprodleně aplikovány na ohrožené systémy či aplikace.

4.12 Zálohování

Zálohování informací v Nemocnici je řešeno centrálně. Požadavky na zálohování a zálohovací mechanismy jsou na základě dokumentovaných podpůrných IT-procesů definovány jejich garanty. Třetí strany musí zajistit, aby:

- byla zálohována všechna důležitá data nezbytná pro zajištění kontinuity provozu jimi spravovaných systémů nebo v rámci jimi poskytovaných IT-služeb, a to vhodnou definicí požadavků na zálohy,
- se na lokálních počítačových stanicích nevyskytovaly žádné informace určené ke sdílení a podléhající centrálnímu zálohování.

Vyžaduje-li to charakter zpracování, jsou individuální zálohy dat na lokálních PC (např. u specifických lokálních agend) řešeny jednotlivě dle požadavků garantů těchto procesů pověřenými zástupci Nemocnice a třetích stran.
Pokud na straně externích dodavatelů existují záložní kopie důležitých informací musí být:

- zabezpečeny před neoprávněným přístupem.

4.13 Požadavky na bezpečnost elektronické dokumentace

Při elektronické komunikaci s Nemocnicí musí třetí strany posuzovat bezpečnostní rizika, která s sebou přináší komunikace prostřednictvím elektronické pošty tak, aby nemohla způsobit přerušení provozu Nemocnice či pád systému nebo služeb, ztrátu nebo kompromitaci neveřejných klasifikovaných informací, infikovat počítačovou síť Nemocnice viry nebo jiným škodlivým SW. Z těchto důvodů jsou u třetích stran uplatňovány následující bezpečnostní požadavky:

- obsah elektronické pošty, včetně příloh v různých formátech přijímaných zpráv, musí být chráněn proti škodlivým kódům účinným antivirovým programem;
- neveřejné klasifikované informace Nemocnice musí být při přenosu prostřednictvím elektronické pošty (nebo obdobné formy komunikace prostřednictvím internetu) chráněny, jinak nesmí být v nezabezpečené formě posílány elektronickou poštou.

Vhodným způsobem ochrany je např. šifrování a použití elektronického podpisu.

4.14 Požadavky na kryptografická opatření

Neveřejné klasifikované informace Nemocnice v elektronické podobě nesmí opustit chráněné prostředí počítačové sítě v otevřené formě. K jejich zabezpečení a přenosu mezi Nemocnicí a třetí stranou musí být určeny smluvně nebo jinou vzájemně dohodnutou formou stanovené systémy, nástroje nebo kryptografické prostředky.

5. Přílohy

Příloha č. 1 - Obsah smlouvy uzavírané s významnými dodavateli
Příloha č. 2 - Zabezpečené oblasti
Příloha č. 3 - Klasifikace aktiv

Příloha č. 1

Obsah smlouvy uzavírané s významnými dodavateli dle přílohy č. 7 VoKB:

a) ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity),
b) ustanovení o oprávnění užívat data,
c) ustanovení o autorství programového kódu, popřípadě o programových licencích,
d) ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu),
e) ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem a nebudou v rozporu s požadavky povinné osoby na dodavatele,
f) ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele povinnou osobou,
g) ustanovení o řízení změn,
h) ustanovení o souladu smluv s obecně závaznými právními předpisy,
i) ustanovení o povinnosti dodavatele informovat povinnou osobu o
    1. kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,
    2. způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy,
    3. významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy se správcem,
j) specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně),
k) specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností),
l) specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem) pravidla pro likvidaci dat,
m) ustanovení o právu jednostranně odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy a
n) ustanovení o sankcích za porušení povinností.

Příloha č. 2 - Zabezpečené oblasti

Fyzické bezpečnostní okruhy:		Požadavky na prvky objektové bezpečnosti:
1. veřejně přístupný prostor	např. veřejně přístupné vstupy (IC), vestibuly, chodby, čekárny, návštěvní místnosti, vnitřní areál	• přístup povolen bez omezení (zaměstnancům, pacientům i veřejnosti) • umístění ICT tak, aby nebyly v dosahu či dohledu nepovolaných osob, pokud k tomu nejsou určeny (jako např. informační panely, obrazovky, kiosky apod.) • uzamykatelný vstup • monitoring kamerovým systémem
2. standardně chráněný prostor	např. běžné administrativní místnosti, zasedací místnosti pro návštěvy, uzavřené čekárny a kabinky pro pacienty, vyšetřovny, sesterny, lůžková oddělení	• přístup povolen pouze určeným zaměstnancům a pozvaným pacientům • vstup návštěv pouze v doprovodu oprávněného zaměstnance • umístění ICT tak, aby nebyly v dosahu/dohledu nepovolaných osob, pokud k tomu nejsou určeny (jako např. informační panely, obrazovky, kiosky apod.) • uzamykatelné úschovné zařízení (zásuvka, skříň vybavená běžným kancelářským zámkem) • uzamykatelný vstup • monitoring kamerovým systémem
3. prostor přístupný pouze zaměstnancům	např. provozní místnosti, zázemí zaměstnanců, kuchyňky, úklidové prostory, zasedací místnosti pro zaměstnance, neveřejný prostor IC, vnitřní koridory Nemocnice	• přístup povolen pouze zaměstnancům, příp. externím poskytovatelům služeb na základě povolení nebo v doprovodu oprávněného zaměstnance • umístění ICT tak, aby nebyly v dosahu/dohledu nepovolaných osob • uzamykatelný vstup (EZS) • monitoring kamerovým systémem
4. nadstandardně chráněný prostor	např. ambulance, ordinace, operační sály, laboratoře, specializovaná pracoviště, kanceláře ICT, zaměstnanců pokladny, personálního oddělení, mzdové účtárny a vedení, pracoviště ostrahy	• přístup povolen pouze určeným zaměstnancům a pozvaným pacientům • vstup návštěv pouze v doprovodu oprávněného zaměstnance • umístění ICT tak, aby nebyly v dosahu/dohledu nepovolaných osob • uzamykatelné úschovné zařízení (zásuvka, registratura, skříň vybavená dozickým zámkem) nebo trezor • uzamykatelný vstup (EZS) • monitoring kamerovým systémem se záznamem (dle směrnice kamerového systému)
5. zabezpečená místnost	např. serverovna, datové centrum, telefonní ústředna,	• protipožární ochrana, teplotní ochrana, • napojení na PCO (ostraha, vrátnice) • uzamykatelný vstup (EZS) • vytápění/klimatizace • UPS/náhradní zdroj energie • teplotní / vlhkostní / pohybová čidla • protipožární čidla a hlásiče, EPS (příp. samozhášecí systém) • kamerový systém se záznamem

Příloha č. 3
Klasifikace aktiv

Úroveň	*Důvěrnost* *Stupeň klasifikace informací*	*Typ informací:*	*Dostupnost*	*Integrita*	*Povolený způsob zacházení:*
Nízká	1. Veřejné informace: (Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy nemocnice.)[7] Není vyžadována žádná ochrana. Likvidace / mazání aktiva na úrovni Nízká.	◆dostupné na stránkách webu nemocnice, ◆povinně zveřejňované informace (dle zák. o svobodném přístupu k informacím, ◆zveřejnitelné informace, jež nevyžadují omezení přístupu.	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne). Pro ochranu dostupnosti je postačující pravidelné zálohování.	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy nemocnice.	◆lze ukládat, přepravovat a sdílet bez omezení, ◆lze publikovat v jakékoliv formě bez omezení, ◆mohou být zálohovány v nechráněné (otevřené) podobě, ◆nemusí být likvidovány (mazány či skartovány) neobnovitelným způsobem.
Úroveň	*Důvěrnost*	*Typ informací:*	*Dostupnost*	*Integrita*	*Povolený způsob zacházení:*

[7] V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP: WHITE.

	Stupeň klasifikace informací				
Střední	2. Interní informace (neveřejné informace interního charakteru): (Aktiva nejsou veřejně přístupná a tvoří know-how nemocnice, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.)[8] Pro ochranu **důvěrnosti** jsou využívány prostředky pro řízení přístupu. Likvidace / mazání aktiva na úrovni Střední.	◆přístupné všem zaměstnancům nemocnice (interní předpisy a dokumenty), ◆nezveřejnitelné informace, jež vyžadují omezení přístupu.	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení zájmů nemocnice. Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva: - může vést k poškození oprávněných zájmů nemocnice, - může se projevit méně závažnými dopady na primární aktiva. Pro ochranu integrity jsou využívány standardní nástroje (např. omezení přístupových práv pro zápis).	◆mohou být ukládány a přenášeny v otevřené podobě pouze uvnitř nemocnice (a jejích ICT), ◆musí být chráněny před neoprávněným přístupem, jsou-li v elektronické formě ukládány na přenosná zařízení a média nebo přepravovány vně nemocnice (a jejích ICT), a to minimálně kvalitním heslem nebo šifrováním, ◆mohou být zálohovány na záložní média v nechráněné podobě, pouze pokud tato média neopustí nemocnice, ◆musí být z jakýchkoliv nosičů dat včetně HDD, které jsou určeny k předání osobám mimo nemocnice bez příslušného oprávnění k nim, likvidovány (tj. mazány či skartovány) bezpečným neobnovitelným způsobem.
Úroveň	*Důvěrnost*	*Typ informací:*	*Dostupnost*	*Integrita*	*Povolený způsob*

[8] V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP: GREEN nebo TLP: AMBER.

	Stupeň klasifikace informací				*zacházení:*
Vysoká	3. Chráněné informace (neveřejné informace charakteru osobních údajů a jiných chráněných informací, jež představují): (Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními.) Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací vnější komunikační sítí jsou chráněny pomocí kryptografických prostředků. Likvidace / mazání aktiva na úrovni Vysoká.	◆osobní údaje zaměstnanců, ◆osobní údaje třetích stran, odběratelů, smluvních partnerů, ◆obchodní tajemství, ◆informace přístupné jednotlivým zaměstnancům nebo určené skupině zaměstnanců nemocnice (zápisy z porad, auditní zprávy, logy apod.).	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů nemocnice. Aktiva jsou považována jako velmi důležitá. Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů nemocnice s podstatnými dopady na primární aktiva. Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených vnějšími komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.	◆musí být vždy chráněny před neoprávněným přístupem (v jakékoliv formě), ◆musí být při ukládání a přenosu ve fyzické podobě chráněny (např. v uzamyk. schránkách, skříních, trezorech), v elektronické formě pak minimálně přístupovými právy, kvalitním heslem nebo šifrováním, a to jak uvnitř nemocnice (a jejích ICT), tak mimo ni, ◆mohou být zálohovány na záložní média pouze v chráněné podobě (omezení přístupu, šifrování), ◆musí být z jakýchkoliv nosičů dat včetně HDD, které jsou určeny k předání osobám (jak interně, tak mimo nemocnice) bez příslušného oprávnění k nim, likvidovány (tj. mazány či skartovány) bezpečným neobnovitelným způsobem.
Úroveň	*Důvěrnost*	*Typ informací:*	*Dostupnost*	*Integrita*	*Povolený způsob*

	Stupeň klasifikace informací				*zacházení:*
Kritická	4. Kritické informace (neveřejné informace charakteru zvláštních kategorií osobních údajů a jiných životně důležitých či důvěrných informací, jež představují): (Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie.)[9] Pro ochranu důvěrnosti je požadována evidence osob, které k aktivům přistoupily, a metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků. Likvidace / mazání aktiva na úrovni Kritická.	◆strategické obchodní tajemství, ◆přístupové údaje (hesla, kódy) k datům a systémům, ◆údaje týkající se dětí, ◆údaje o zdravotním stavu pacientů i zaměstnanců, ◆údaje týkající se rozsudků v trestních věcech a trestných činů, ◆údaje o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, ◆údaje o členství v odborech, genetické údaje, biometrické údajů za účelem jedinečné identifikace fyzické osoby, ◆údaje o sexuálním životě nebo sexuální orientaci.	Narušení dostupnosti aktiva není přípustné, i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení zájmů nemocnice. Aktiva jsou považována za kritická. Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů nemocnice s přímými a velmi vážnými dopady na primární aktiva. Pro ochranu **integrity** jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (např. pomocí technologie digitálního podpisu).	◆musí být vždy chráněny před neoprávněným přístupem (v jakékoliv formě), ◆musí být při ukládání a přenosu ve fyzické podobě chráněny (např. v uzamykatelných schránkách, skříních, trezorech), v elektronické formě pak minimálně přístupovými právy, kvalitním heslem nebo šifrováním, a to jak uvnitř nemocnice (a jejích ICT), tak mimo ni, ◆mohou být zálohovány na záložní média pouze v chráněné podobě (omezení přístupu, šifrování), ◆musí být z jakýchkoliv nosičů dat včetně HDD, které jsou určeny k předání osobám (jak interně, tak mimo nemocnice) bez příslušného oprávnění k nim, likvidovány (tj. mazány či skartovány) bezpečným neobnovitelným způsobem.

[9] V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP: RED nebo TLP: AMBER.