|  |  |  |
| --- | --- | --- |
| **Typ řídicího dokumentu** | | LOGO |
| Číslo: **AAA XXX** | Vydání: X | **Nemocnice** |
| Datum: 00. 00. 0000 |  | nemocnice Středočeského kraje |

|  |
| --- |
| **Směrnice AAA XXX**  **politika bezpečnosti informací** |

Účinnost dokumentu od: **00. 00. 0000**

|  |  |  |
| --- | --- | --- |
| Zpracoval: | Titul Jméno Příjmení  Funkce | Podpis: …………………….. |
| Garant: | Titul Jméno Příjmení  Funkce | Podpis: …………………….. |
| Správce dokumentu: | Titul Jméno Příjmení  Funkce | Podpis: …………………….. |
| Schválil: | Titul Jméno Příjmení  Funkce | Podpis: …………………….. |

**O**bsah

[Čl. 1 Politika bezpečnosti informací 5](#_Toc73083873)

[Čl. 2 Zásady bezpečnosti informací 5](#_Toc73083874)

[Příloha 1. Politika systému řízení bezpečnosti informací 6](#_Toc73083875)

[Čl. 1 Úvodní ustanovení 6](#_Toc73083876)

[Čl. 2 Působnost 6](#_Toc73083877)

[Čl. 3 Cíle, principy a potřeby SŘBI 6](#_Toc73083878)

[Čl. 4 Rozsah a hranice SŘBI 7](#_Toc73083879)

[Čl. 5 Pravidla a postupy pro řízení dokumentace SŘBI 8](#_Toc73083880)

[Čl. 6 Pravidla a postupy pro řízení zdrojů a provozu SŘBI 9](#_Toc73083881)

[Čl. 7 Pravidla a postupy pro provádění auditů SŘBI 9](#_Toc73083882)

[Čl. 8 Pravidla a postupy pro přezkoumání SŘBI 10](#_Toc73083883)

[Čl. 9 Pravidla a postupy pro přijatá opatření a zlepšování SŘBI 10](#_Toc73083884)

[Příloha 2. Bezpečnostní opatření pro uživatele 12](#_Toc73083885)

[Čl. 1 Úvodní ustanovení 12](#_Toc73083886)

[Čl. 2 Působnost 12](#_Toc73083887)

[Čl. 3 Zásady ochrany informací 12](#_Toc73083888)

[Čl. 4 Klasifikace aktiv 12](#_Toc73083889)

[Čl. 5 Bezpečnostní povědomí 13](#_Toc73083890)

[Čl. 6 Řízení přístupu 13](#_Toc73083891)

[Čl. 7 Kryptografická ochrana 15](#_Toc73083892)

[Čl. 8 Fyzická bezpečnost 15](#_Toc73083893)

[Čl. 9 Provoz a komunikace 15](#_Toc73083894)

[Čl. 10 Škodlivý kód 16](#_Toc73083895)

[Čl. 11 Bezpečnostní incident 16](#_Toc73083896)

[Příloha 3. Bezpečnostní opatření pro IT pracovníky 17](#_Toc73083897)

[Čl. 1 Úvodní ustanovení 17](#_Toc73083898)

[Čl. 2 Působnost 17](#_Toc73083899)

[Čl. 3 Bezpečnostní požadavky na provoz a správu IT technologií 17](#_Toc73083900)

[Čl. 4 Klasifikace aktiv 17](#_Toc73083901)

[Čl. 5 Bezpečnostní povědomí 18](#_Toc73083902)

[Čl. 6 Řízení přístupu 18](#_Toc73083903)

[Čl. 7 Kryptografická ochrana 20](#_Toc73083904)

[Čl. 8 Fyzická bezpečnost 20](#_Toc73083905)

[Čl. 9 Provoz a komunikace 21](#_Toc73083906)

[Čl. 10 Dodavatelé 22](#_Toc73083907)

[Čl. 11 Kontinuita činností 22](#_Toc73083908)

[Čl. 12 Soulad s požadavky 23](#_Toc73083909)

[Příloha 4. Přechodná ustanovení 24](#_Toc73083910)

[Čl. 1 Úvodní ustanovení 24](#_Toc73083911)

[Čl. 2 Působnost článku politiky či ustanovení 24](#_Toc73083912)

[Příloha 5. Přehled související legislativy 25](#_Toc73083913)

**Související interní předpisy**

AAA XXX Organizační řád

AAA XXX Spisový a skartační řád

AAA XXX Politika fyzické bezpečnosti

AAA XXX Politika ochrany osobních údajů

AAA XXX Název dokumentu

**Přílohy**

Příloha č. 1: Politika systému řízení bezpečnosti informací

Příloha č. 2: Bezpečnostní opatření pro uživatele

Příloha č. 3: Bezpečnostní opatření pro IT pracovníky

Příloha č. 4: Přehled související legislativy

**Použité zkratky**

DPO Pověřenec pro ochranu osobních údajů

DRP Plán obnovy

HW Hardware

IT Informační technologie

KB Kybernetická bezpečnost

NDA Smlouva o zachování mlčenlivosti

NÚKIB Národní úřad pro kybernetickou a informační bezpečnost

SLA Dohoda o úrovni poskytovaných služeb

SŘBI Systém řízení bezpečnosti informací

SW Software

ZZZZ definice termínu

ZZZZ definice termínu

ZZZZ definice termínu

ZZZZ definice termínu

**Preambule**

Politika bezpečnosti informací stanovuje minimální požadavky pro oblast bezpečnosti informací pro nemocnice zřizované Středočeským krajem. Nemocnice může v rámci přizpůsobení dokumentu jednotlivé požadavky i dále zpřísnit.

## Čl. 1 Politika bezpečnosti informací

1. Nemocnice XXXXXXXXXX (dále jen Nemocnice) je akciovou společností založenou Středočeským krajem za účelem zajištění zdravotní péče občanům ve formě plnění závazku veřejné služby v oblasti poskytování zdravotních služeb ve smyslu zákona č. 372/2011 Sb. a v rozsahu uzavřených smluv se zdravotními pojišťovnami dle zákona č. 48/1997 Sb.
2. Cílem Nemocnice je zajištění dostupnosti a bezpečnosti dat a osobních údajů nezbytných pro poskytování služeb pro pacienty. Tento je naplňován provozováním, kontrolováním, údržbou a neustálým zlepšováním Systému řízení bezpečnosti informací (dále jen „SŘBI“) s ohledem na rizika a zákonné a požadavky dopadající na Nemocnici v oblasti bezpečnosti informací. Jeho politiku stanovuje příloha č. 1.
3. Odpovědnost za bezpečnost informací nese nejen vrcholové vedení Nemocnice, ale každý jednotlivý uživatel informačního systému Nemocnice – zaměstnanec či dodavatel. Jednotlivá opatření s ohledem na pracovní zařazení stanovují přílohy č. 2 a 3.
4. Ochrana osobních údajů je zajištěna v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016. Nemocnice má stanoveného Pověřence pro ochranu osobních údajů (DPO) a postupuje v souladu s Politikou ochrany osobních údajů
5. Přechodná ustanovení v příloze 4 vymezují platnost politiky vůči aktuálnímu nastavení informačního systému Nemocnice a stanovují období, kdy bude politika plně prosazena.

## Čl. 2 Zásady bezpečnosti informací

1. Bezpečnost dat je závislá zejména na zachování důvěrnosti osobních zdravotních údajů pacientů, osobních dat zaměstnanců a pracovníků našich dodavatelů. Dodržujeme zásadu mlčenlivosti a máme nastavena pravidla pro osobní, písemnou a elektronickou komunikaci.
2. Dostupnost správných informací je rozhodující pro zajištění včasné a účinné zdravotní péče. Při zadávání do systémů ověřujeme správnost informace a před výkonem zákroků v rámci zdravotních služeb zajišťujeme poučení a informovaný souhlas pacienta.
3. Bezpečnostní opatření stanovená přílohami politiky chrání procesy před selháním a informace před zcizením a následným zneužitím. Dodržujeme stanovená opatření v rámci každodenních rutinních činností při poskytování zdravotních služeb pacientům.
4. Klíčovým prvkem je zvyšování povědomí o existujících bezpečnostních hrozbách. Jsme si vědomi bezpečnostních hrozeb a podílíme se na dodržování stanovených opatření a vzdělávání v oblasti bezpečnosti informací.
5. Porušení opatření stanovených přílohami politiky je bezpečnostním incidentem a může mít závažné důsledky nejen v oblasti bezpečnosti informací. Setkáme-li se s takovou situací, důsledně postupujeme dle stanovených pravidel pro tyto případy.
6. Sledování a vyhodnocování rizik a hrozeb je nedílnou součástí každé aktivity zajišťování bezpečnosti. Stanovené opatření odpovědní pracovníci pravidelně přehodnocují nejen s ohledem na aktuální hrozby a rizika, ale i na podněty ke zlepšení.
7. Pro zajištění bezpečnosti informací je třeba vytvořit podmínky a zajistit nezbytné zdroje. Plánované náklady jsou financovány vyváženě a odpovídají aktuální míře rizika při dosažení efektivnosti takto vynaložených zdrojů.

# Příloha 1. Politika systému řízení bezpečnosti informací

## Čl. 1 Úvodní ustanovení

1. Nemocnice XXXXXXXXXX (dále jen Nemocnice) je akciovou společností založenou Středočeským krajem za účelem zajištění zdravotní péče občanům ve formě plnění závazku veřejné služby v oblasti poskytování zdravotních služeb ve smyslu zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování, a v rozsahu uzavřených smluv se zdravotními pojišťovnami dle zákona č. 48/1997 Sb. o veřejném zdravotním pojištění. Organizační strukturu stanovuje Organizační řád.
2. Hlavním předmětem činnosti Nemocnice je poskytování komplexní léčebné, diagnostické a preventivní zdravotnické péče pacientům. Doplňkovými předměty činnostmi jsou masérské, rekondiční a regenerační služby, hostinská činnost, nakládání s nebezpečnými odpady, čištění a praní textilu a oděvů a péče o děti do tří let věku v denním režimu.
3. Tyto služby realizuje Nemocnice v X vlastních/pronajatých areálech/budovách, za využití informací o pacientech a klientech zpracovávaných v informačních systémech.
4. Nemocnice má zaveden systém řízení bezpečnosti informací (díle jen SŘBI) pro zajištění dostupnosti a bezpečnosti dat a osobních údajů nezbytných pro poskytování kvalitních služeb v oblasti komplexní léčebné, diagnostické a preventivní zdravotnické péče pacientům a dalších doplňkových služeb klientům. SŘBI zajišťuje adekvátní ochranu aktiv z pohledu možného narušení jejich důvěrnosti, integrity nebo dostupnosti a minimalizaci ztrát v důsledku kybernetických incidentů.

## Čl. 2 Působnost

1. Působnost politiky se vztahuje na všechny zaměstnance a externí pracovníky zpracovávající informace, s využitím informačních systémů Nemocnice nebo jiných prostředků výpočetní techniky ve správě Nemocnice.

## Čl. 3 Cíle, principy a potřeby SŘBI

1. Cíle SŘBI průběžně vycházejí z jednotlivých bezpečnostních požadavků v rámci procesu řízení kybernetické bezpečnosti. Musí být měřitelné, jsou průběžně sledovány a vyhodnocovány. Jsou schváleny Výborem KB a za přípravu je odpovědný Manažer KB. Na přípravě cílů se podílí Garanti aktiv, kteří jsou odpovědní za plnění bezpečnostních opatření. Cíle jsou plněny formou aktivit či dílčích projektů. Každý cíl má stanoveno:

1) co bude vykonáno,

2) jaké zdroje budou využity,

3) kdo bude za realizaci odpovědný,

4) kdy bude dokončen,

5) jak bude vyhodnocen.

1. Principy SŘBI stanovující směr rozvoje procesu řízení kybernetické bezpečnosti Nemocnice a přezkoumávané Výborem KB jsou:

1) zajištění souladu s právními předpisy,

2) zvyšování bezpečnostního povědomí uživatelů,

3) systematické zlepšování procesů a opatření,

4) zajištění nezbytné ochrany důvěrnosti, integrity a dostupnosti zpracovávaných informací.

1. Potřeby SŘBI s ohledem na zajištění dostupnosti a bezpečnosti dat a osobních údajů:

1) zásady ochrany informací jsou uplatňovány ve všech procesech i každodenních činnostech, ochrany hmotných i nehmotných aktiv a nedílnou součástí kvality služeb Nemocnice v oblasti komplexní léčebné, diagnostické a preventivní zdravotnické péče poskytovaných pacientům a dalších doplňkových služeb poskytovaných klientům,

2) stanovené bezpečnostní zásady, pravidla, postupy a přijatá opatření k zajištění jejich realizace v jednotlivých oblastech jsou průběžně vyhodnocovány a aktualizovány s ohledem na měnící se prostředí Nemocnice, nové hrozby, konkrétní bezpečnostní situaci, vývoj a dostupnost nových bezpečnostních metod, nástrojů a prostředků,

3) důsledné a úspěšné prosazování stanovených bezpečnostních zásad, pravidel a postupů je založeno na stanovení individuální odpovědnosti konkrétních osob, budovaném a kontinuálně udržovaném vysokém bezpečnostním povědomí,

4) přijatá opatření preventivně omezují působení hrozeb na aktiva a jsou finančně méně náročná než odstraňování následků a náprava způsobených škod,

5) přijatá opatření jsou úměrná míře reálných rizik, hodnotě chráněných aktiv a výši škod, které by mohly vzniknout v důsledku jejich nepřijetí,

6) přijatá opatření jsou schopna účinně detekovat kybernetickou bezpečnostní událost a minimalizovat její dopady,

7) přijatá opatření dosahují účinnosti a efektivnosti jednotným přístupem prosazování politiky a použití bezpečnostních prvků na všech úrovních organizační struktury Nemocnice,

8) stav a účinnost přijatých opatření, objektivní měření, výstupy analýzy rizik, výsledky realizovaných auditů, kontrol a poučení se z bezpečnostních incidentů jsou podkladem pro neustálé zlepšování a zvyšování výkonnosti systému řízení bezpečnosti informací Nemocnice.

## Čl. 4 Rozsah a hranice SŘBI

1. Do rozsahu působnosti SŘBI spadají všechny procesy a činnosti, jejich podpůrné informační systémy, lokality, kde jsou tyto procesy realizovány a další aktiva Nemocnice nutná k zajištění poskytování komplexní léčebné, diagnostické a preventivní zdravotnické péče pacientům a dalších doplňkových služeb klientům:

1) areál/budovy Nemocnice na adrese Adresa,

2) útvary Nemocnice vymezené dle Organizačního řádu,

3) informační systémy zajišťující podporu procesů a zpracování dat Nemocnice je tvořen Informačním systém,

4) externími subjekty jsou pacienti a klienti nemocnice, dodavatelé a další osoby dle příslušných zákonů (správní orgány, orgány ochrany veřejného zdraví, zdravotní pojišťovny, Státní ústav pro kontrolu léčiv, atd.).

1. Hranice SŘBI tvoří vstupní a výstupní místa mezi informačními systémy Nemocnice a externími počítačovými a komunikačními sítěmi, například Internetem. V případě vzdálených přístupů jsou hraničními ta rozhraní, která jsou umístěna v areálech či budovách Nemocnice respektive třetích stran poskytujících Nemocnici outsourcingové služby pro provoz informačního systému.

## Čl. 5 Pravidla a postupy pro řízení dokumentace SŘBI

1. Pravidla a postupy pro řízení dokumentace SŘBI jsou stanovena Spisovým a skartačním řádem. Bezpečnostní dokumentace je dostupná všem uživatelům informačního systému Nemocnice na intranetu a to v nezbytném rozsahu, s nímž musejí být pro jimi zastávanou roli seznámeni. Není-li uvedeno jinak, je Politika bezpečnosti informací klasifikována stupněm Interní a ostatní bezpečnostní dokumentace stupněm Chráněný. Bezpečnostní dokumentace je schvalována či vzata na vědomí Výborem KB, za přípravu a revize je odpovědný Manažer KB a na její přípravě se podílí Garanti aktiv.
2. Bezpečnostní dokumentaci Nemocnice tvoří:

1) Politika bezpečnosti informací včetně příloh,

2) Provozní bezpečnostní dokumentace (prohlášení o aplikovatelnosti, plán rozvoje bezpečnostního povědomí, plán zvládání rizik, zpráva z hodnocení aktiv a rizik, zpráva z auditu, zpráva z přezkoumání SŘBI),

3) Řízené záznamy o bezpečnostně relevantních událostech (evidence změn, evidence výjimek, konfigurační databáze, adresní plán, komunikace s dotčenými správními orgány)

1. Manažer KB je odpovědný za přezkoumání všech výjimek a ve spolupráci s příslušným žadatelem musí připravit efektivní plán na zvládání a řešení výjimky, která je v souladu platným plánem zvládání rizik. Evidence výjimek obsahuje:

1) identifikaci žadatele o výjimku,

2) identifikaci bezpečnostních pravidel, která není možné dodržovat,

3) vysvětlení, proč není možné pravidla dodržovat a je nutná výjimka,

4) stanovení časového období, na které je výjimka schválená,

5) dočasná opatření, která omezují nežádoucí dopady.

1. Řízení aktiv v podobě zdravotní dokumentace v elektronické i tištěné forměv je upraveno řídícími dokumenty a pokyny vydávanými Zástupcem ředitele pro zdravotní péči. Za vedení evidence aktiv v rámci jednotlivých informačních systémů jsou odpovědni Garanti aktiv.:
2. Šíření a používání aktiv je omezeno dle příslušného stupně. Přípustné způsoby nakládání s klasifikovanými informacemi jsou uvedeny v článku 4 přílohy 2 Bezpečnostní opatření pro uživatele.

## Čl. 6 Pravidla a postupy pro řízení zdrojů a provozu SŘBI

1. Zdroje potřebné pro ustanovení, implementování, udržování a neustálé zlepšování SŘBI Nemocnice musí být plánovány a alokovány. Za zajištění zdrojů je odpovědný Předseda představenstva, za jejich plánování a alokaci příslušní vedoucí pracovníci, do jejichž kompetence dle Organizačního řádu uvedené zdroje spadají.
2. Lidské zdroje pro výkon rolí SŘBI zahrnují:

1) Manažer KB – pověřený pracovník Nemocnice či služba outsourcingu výkonu role v rozsahu § 7, odst. 1 a 2 vyhlášky č. 82/2018 Sb., role není slučitelná s rolemi odpovědnými za provoz informačních systémů, role je v kompetenci Provozního ředitele,

2) Garant aktiva – pověřený pracovník Nemocnice k výkonu role v rozsahu § 7, odst. 3 vyhlášky č. 82/2018 Sb., role je v kompetenci Provozního ředitele,

3) Auditor KB – pověřený pracovník Nemocnice či služba outsourcingu výkonu role v rozsahu § 7, odst. 4 vyhlášky č. 82/2018 Sb., role není slučitelná s rolemi Manažer KB, Garant aktiva a rolemi odpovědnými za provoz informačních systémů, role je v kompetenci Ředitele auditu.

1. Podmínky pro odbornou způsobilost a praxi jsou stanoveny v příloze č. 6 vyhlášky č. 82/2018 Sb. O jmenování do role rozhoduje Předseda představenstva na návrh příslušného vedoucího pracovníka, do jejichž kompetence v rámci definované dle Organizačního řádu uvedená role spadá.
2. Za zabezpečení finančních zdrojů je odpovědný Finanční ředitel. Výbor KB předkládá každoročně Finančnímu řediteli odhad finančních zdrojů nezbytně nutných pro správný a efektivní provoz SŘBI Nemocnice.
3. Za zabezpečení technických zdrojů je odpovědný Ředitel IT. Výbor KB předkládá každoročně Řediteli IT odhad technických zdrojů nezbytně nutných pro správný a efektivní provoz SŘBI Nemocnice.
4. Za celkové řízení a rozvoj kybernetické bezpečnosti Nemocnice je odpovědný Výbor KB. Jednotlivé činnosti zahrnují tvorbu rámce kybernetické bezpečnosti, směrování a zásad kybernetické bezpečnosti, kontrolu aktuálního stavu kybernetické bezpečnosti a zjišťování, zda dochází k naplňování plánovaných cílů. Je ustanoven v souladu s Organizačním řádem. Členy Výboru KB jsou:

1) Provozní ředitel,

2) Manažer KB,

3) Garant aktiva.

## Čl. 7 Pravidla a postupy pro provádění auditů SŘBI

1. Nezávislé přezkoumání, audit a kontrolu souladu s bezpečnostní politikou, provozními standardy IT a platnou legislativou zajišťuje Auditor KB na základě plánu auditů schváleného vedením Nemocnice.
2. Audit je prováděn v celém rozsahu SŘBI nejméně jednou za dva roky a při významných změnách v rámci jejich rozsahu. Cílem auditu je nezávisle přezkoumat a ověřit, zda SŘBI Nemocnice:

1) vyhovuje požadavkům stanoveným legislativou,

2) vyhovuje požadavkům stanoveným Politikou bezpečnosti informací a postupům řízení KB,

3) je efektivně implementován a provozován.

1. Audit vykonává pověřený pracovník Nemocnice či externí dodavatel služby outsourcingu výkonu role v rozsahu § 7, odst. 4 vyhlášky č. 82/2018 Sb. Podmínky pro odbornou způsobilost a praxi jsou stanoveny v příloze č. 6 vyhlášky č. 82/2018 Sb. O jmenování do role rozhoduje Předseda představenstva na návrh Ředitele auditu. Není-li Auditorem KB rozhodnuto jinak, jsou zpráva z auditu KB a nálezy auditu KB klasifikovány stupněm Chráněný.

## Čl. 8 Pravidla a postupy pro přezkoumání SŘBI

Výbor KB musí nejméně jednou ročně provést přezkoumání SŘBI.

1. Manažer KB předkládá Výboru KB jednou ročně podklady pro přezkoumání SŘBI, která obsahují:

1) vyhodnocení opatření z předchozího přezkoumání SŘBI,

2) identifikace změn a okolností mající vliv na SŘBI,

3) zpětná vazba o výkonosti SŘBI, včetně trendů spojených s:

a) riziky a přijatými opatřeními,

b) výsledky monitorování a měření,

c) výsledky auditů KB,

d) naplněním cílů SŘBI,

4) výsledky hodnocení rizik a stav zvládání rizik,

5) identifikace možností pro neustálé zlepšování,

6) doporučení potřebných rozhodnutí, stanovení opatření a osob zajišťujících výkon jednotlivých činností.

1. Výstupy z přezkoumání SŘBI musí obsahovat rozhodnutí Výboru KB, které se vztahují k neustálému zlepšování a potřebám změn SŘBI včetně jejich priorit. Manažer KB zaznamenává učiněná rozhodnutí a další závěry do zápisu z jednání Výboru KB a je odpovědný za přenesení všech rozhodnutí Výboru KB do plánu zvládání rizik.

## Čl. 9 Pravidla a postupy pro přijatá opatření a zlepšování SŘBI

1. Rozvoj SŘBI je založen na přijatých opatřeních a neustálém zlepšování.
2. Při identifikaci rizika Manažer KB nebo jím pověřená osoba musí:

1) reagovat na riziko, a pokud je to aplikovatelné:

a) přijmout opatření k řízení a nápravě rizika,

b) zabývat se následky,

2) vyhodnotit potřebu pro opatření k odstranění příčin rizika, aby se znovu nevyskytlo prostřednictvím:

a) přezkoumání rizika,

b) určení příčin rizika,

c) určení, zda existují podobná rizika nebo by se mohly potenciálně vyskytnout,

3) implementovat jakákoliv potřebná opatření,

4) přezkoumat efektivnost každého přijatého opatření,

5) provést změny SŘBI, pokud je to nezbytné.

1. Přijatá opatření musí být přiměřená dopadům rizik, kterým čelí. Manažer KB musí zaznamenat:

1) podstatu rizika a každého následného přijatého opatření,

2) výsledky každého přijatého opatření.

1. Manažer KB je odpovědný za identifikací podnětů pro neustálé zlepšování. A to se zřetelem na vhodnost, přiměřenost, efektivnost a určení priority jednotlivých činností. Priorita každé činnosti musí odrážet přínosy činnosti neustálého zlepšování s ohledem na:

1) plnění cílů SŘBI,

2) zvládání rizik, která překročila kritéria pro přijatelnost rizik,

3) ošetření výjimek vůči politikám a postupům řízení bezpečnosti,

4) zvýšení účelnosti a efektivnosti opatření SŘBI,

5) úsporu zdrojů potřebných pro řízení SŘBI.

1. Činnosti neustálého zlepšování musí být zahrnuty do plánu zvládání rizik.

# Příloha 2. Bezpečnostní opatření pro uživatele

## Čl. 1 Úvodní ustanovení

1. Nemocnice XXXXXXXXXX (dále jen Nemocnice) v rámci SŘBI stanovuje bezpečnostní pravidla pro uživatele a externí pracovníky k zajištění bezpečnosti informací a kontinuity činností Nemocnice.

## Čl. 2 Působnost

1. Působnost směrnice se vztahuje na všechny zaměstnance a externí pracovníky zpracovávající informace, využívající informační systémy nebo jiné prostředky Nemocnice.
2. Zaměstnanci a externí pracovníci, kterým jsou přidělena administrátorská oprávnění k zařízení ve vlastnictví Nemocnice, k systému či aplikaci zpracovávajícím informace Nemocnice či zřízením připojovaným do interní sítě Nemocnice (přímo či připojovaným prostřednictvím vzdáleného přístupu) jsou povinni dodržovat relevantní ustanovení uvedené v příloze 3 Bezpečnostní opatření pro IT pracovníky.

## Čl. 3 Zásady ochrany informací

1. Informace jsou důležitými aktivy Nemocnice, které je potřeba chránit před jejich ztrátou (smazáním, zničením), prozrazením nebo nežádoucím pozměněním.
2. Dodržování následujících zásad ochrany informací má za úkol napomáhat zaměstnancům i externím pracovníkům chránit své soukromí i data Nemocnice.

## Čl. 4 Klasifikace aktiv

1. Pravidla pro používání aktiv kategorie informace vycházejí ze zákonných požadavků na jejich ochranu, jejich významu a kategorie v případě osobních údajů. Nemocnice využívá čtyř-stupňovou klasifikační stupnici odpovídající vyhlášce č. 82/2018 Sb:

|  |  |
| --- | --- |
| Klasifikační stupeň | Označení dle vyhlášky č. 82/2018 Sb. |
| Veřejné | Nízká |
| Interní | Střední |
| Chráněné | Vysoká |
| Přísně chráněné | Kritická |

1. Klasifikace je povinná pro veškeré informace a data. Je realizována jejich vlastníky. Informace klasifikované jako Chráněné se neoznačují. Jako Interní lze označit pouze dokumenty a data, které jsou anonymizovány, nejsou zdravotnickou dokumentací či neobsahují osobní údaje pacientů a klientů. Stupeň Veřejné jsou oprávnění používat pouze pracovníci útvaru Komunikace.
2. Pravidla pro jednotlivé způsoby nakládání s klasifikovanými informacemi s ohledem na jejich stupeň:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Veřejné | Interní | Chráněné | Přísně chráněné |
| Ukládání | Bez omezení | Jen uživatelé s přístupy do interní sítě | Jen oprávnění uživatelé a správci systému | Šifrované, jen oprávnění uživatelé, nikoliv správci systému |
| Předávání v Nemocnici | Bez omezení | Všichni zaměstnanci a dodavatelé | Na základě potřeby přístupu k informaci | Jen po schválení vlastníka informace |
| Předávání mimo Nemocnici | Bez omezení | NDA | NDA s významnou sankcí, šifrování | NDA s vymíněním zvláštní ochrany, šifrování |
| Zasílání | Bez omezení | Oprávněný příjemce | Oprávněný příjemce, ochrana heslem | Šifrované, klíč předáván odděleně |
| Likvidace | Bez omezení | Běžný výmaz informace | Opakovaný přepis informace | Fyzická likvidace datových nosičů |
| Zveřejnění | Bez omezení | Na základě schválení útvaru Komunikace | Jen anonymizované informace a po schválení Garanta | Pouze na základě soudního rozhodnutí |

## Čl. 5 Bezpečnostní povědomí

1. Požadavky na úvodní a pravidelná školení uživatelů a pracovníků obsazených do bezpečnostních rolí stanovuje plán rozvoje bezpečnostního povědomí. Za plánování a realizaci školení odpovídá útvar HR.
2. Zaměstnanci a externí pracovníci jsou v okamžiku nástupu prokazatelně seznámeni se svými povinnostmi v oblasti informační bezpečnosti. Nejpozději k okamžiku nástupu a před převzetím uživatelských oprávnění do informačního systému Nemocnice jsou povinni absolvovat úvodní zaškolení v oblasti bezpečnosti informací formou absolvování elektronického kurzu a zakončeného testem. Na základě úspěšného absolvování je uživateli vystaven certifikát. Minimální zásady obsahuje elearningový kurz základů kybernetické bezpečnosti s názvem Dávej kyber! poskytovaný NÚKIB.
3. Zaměstnanci a externí pracovníci jsou v souladu s požadavky pracovní pozice povinni absolvovat průběžné školení v oblasti bezpečnosti informací a to nejméně jedenkrát ročné. Sledování a organizaci pravidelných školení zajišťuje útvar HR.

## Čl. 6 Řízení přístupu

1. Přístup k informační systémům je přidělen pouze oprávněným uživatelům na základě úspěšného ověření (přihlašovacím jménem a heslem, čipovou kartou nebo bezpečnostním tokenem a pinem).
2. V Nemocnici je uplatňován princip neodmítnutelnosti odpovědnosti. To znamená, že uživatel odpovídá za všechny skutky, které byly vykonány jeho účtem, kdy byl informačním systémem Nemocnice úspěšně ověřen (přihlašovacím jménem a heslem, čipovou kartou nebo bezpečnostním tokenem a pinem).
3. V případě podezření na kompromitaci hesla (jeho prozrazení, odposlechnutí, či uhodnutí jinou osobou) je uživatel povinen neodkladně provést změnu hesla a tuto skutečnost neprodleně hlásit na Service Desku jako bezpečnostní incident.
4. Potřebná přístupová oprávnění jsou uživateli přidělena dle jeho pracovního zařazení. Přihlašovací jméno a heslo pro první přihlášení je uživateli přiděleno útvarem IT.
5. Uživatel je povinen si heslo po prvním přihlášení změnit a držet jej v tajnosti. To znamená nikomu jej nesdělovat, neponechávat napsané v místech s přístupem dalších osob, neukládat do souboru volně přístupného dalším uživatelům.
6. Při ukládání hesel na počítači či mobilním telefonu je třeba využít k tomu určenou aplikaci správce hesel s odpovídajícím zabezpečením (šifrování, vícefaktorové ověření uživatele, atp.).
7. O změnu oprávnění si uživatel může požádat prostřednictvím žádosti v Service Desku. Žádost o rozšíření oprávnění je vždy schvalována vedoucím pracovníkem žadatele a garantem oprávnění, o které je žádáno. Žádost o odebrání oprávnění je vždy schvalována vedoucím pracovníkem či odpovědným pracovníkem útvaru HR.
8. Při změně pracovní pozice jsou ke dni účinnosti změny uživateli původní oprávnění odebrána a nastavena nová oprávnění v souladu s novým pracovním zařazením.
9. Ke dni bezprostředně následujícím den ukončení pracovního poměru či smluvního vztahu s uživatelem jsou přístupová oprávnění uživatele z informačního systému nemocnice odebrána a účet zablokován.
10. Přihlašovací heslo je nutné volit tak, aby nebylo snadno uhodnutelné a současně bylo dostatečně odolné proti prolomení při kybernetickém bezpečnostním útoku.
11. Pro heslo nesmí být použity snadno identifikovatelná jména (vlastní, rodičů, sourozenců, dětí, domácích zvířat apod.), data narození, názvy měsíců, a jiné snadno uhodnutelné kombinace.
12. Pro hesla do informačních systémů Nemocnice platí tyto požadavky:

|  |  |
| --- | --- |
| Minimální délka: | 12 znaků |
| Minimální platnost: | 30 minut |
| Komplexnost: | Heslo musí obsahovat minimálně 3 z těchto požadavků:  - jedno velké písmeno,  - jedno malé písmeno,  - jednu číslici,  - jeden speciální znak (. , - \* \_ + # $ apod.). |
| Povinná změna: | Minimálně 1x za 18 měsíců |
| Opakovatelnost: | Stejné heslo se nesmí opakovat min. 12 změn zpět. |

1. Je efektivní tvořit hesla na základě fráze, například:

Snědl Tomáš 8 knedlíků nebo 14 ? → Heslo: ST8kn14?

1. Zařízení Nemocnice (počítače, notebooky, tablety, chytré mobilní telefony, …) jsou po 15/30/… minutách nečinnosti uživatele automaticky uzamčeny. Pro jejich opětovné použití je vyžadováno opakované úspěšného ověření již přihlášeného uživatele (přihlašovacím jménem a heslem, čipovou kartou nebo bezpečnostním tokenem a pinem).

## Čl. 7 Kryptografická ochrana

1. Slouží k ochraně informací, pro jejich bezpečné uložení nebo přenos přes datové sítě. Nastavení kryptografických prostředků je zajištěno útvarem IT, uživatelům je toto nastavení zakázáno jakkoliv měnit, upravovat či kryptografickou ochranu vypínat.
2. Doplnit konkrétní SW a instrukce k jeho použití pro Vzdálený přístup pomocí VPN – viz pracovní postupy na Intranetu
3. Doplnit konkrétní SW a instrukce k jeho použití pro šifrování souborů – viz pracovní postupy na Intranetu
4. Pro zaslání klasifikovaných informací elektronické pošty je nutné soubory zašifrovat. Adresátovi sdělte heslo odděleně od zprávy, k níž je připojen chráněný soubor (např. telefonicky či SMS).
5. Doplnit konkrétní SW a instrukce k jeho použití pro elektronický podpis – viz pracovní postupy na Intranetu

## Čl. 8 Fyzická bezpečnost

1. Zajištění fyzické bezpečnosti budov a areálu Nemocnice je realizováno útvarem FM. Uživatelé jsou povinni respektovat ustanovení politiky fyzické bezpečnosti:
2. kanceláře, místnosti zdravotnického provozu a zde umístěná zařízení Nemocnice jsou zabezpečeny s využitím klíčového režimu či hesel,
3. klíče jsou k dispozici zaměstnancům Nemocnice na základě pracovního zařazení či vykonávané funkce,
4. veřejnost má přístup pouze do určených prostor (např. informační kancelář, recepce, čekárna, vyšetřovna, pokladna, atp.), a
5. v ostatních prostorech (např. laboratoře, lékárna, sesterna, kanceláře, atp.) je pohyb cizích osob možný pouze v doprovodu odpovědného zaměstnance nemocnice a nevylučují-li to zvláštní předpisy (např. Směrnice pro nakládání s nebezpečným odpadem).
6. Zaměstnanci a externí pracovníci, kterým byla svěřena výpočetní technika či mobilní zařízení (notebook, tablet, telefon) jsou povinni je zajistit před jejich zcizením (uzamčení bezpečnostním lankem, neponechávat bez dozoru v prostorech s pohybem dalších osob např. v automobilu, apod.).
7. Pro zajištění bezpečnosti informací je prosazováno dodržování politiky čistého stolu. Je zakázáno ponechávat tištěné materiály a jiná mobilní zařízení obsahující klasifikované informace volně položené na pracovním stole, přihlášené či neuzamčené bez dozoru.

## Čl. 9 Provoz a komunikace

1. Zabezpečení provozu a komunikace je zajišťováno útvarem IT. Uživatelům je zakázáno měnit bezpečnostní nastavení a instalovat neschválený software.

## Čl. 10 Škodlivý kód

1. Škodlivý kód představuje velké riziko ohrožení informací. Příkladem je situace, kdy je v  příloze zprávy elektronické pošty obsažen neznámý soubor. V případě napadení počítače škodlivým kódem může tento dělat vše, co je povoleno uživateli, který je právě přihlášen.
2. Na ochranu před škodlivým kódem je na výpočetní techniku útvarem IT instalována antivirová ochrana. Uživatelům je zakázáno jakkoliv měnit nastavení antiviru, či jej vypínat.
3. Zvýšená obezřetnost je třeba při stahování různých souborů a otevírání příloh elektronické pošty v podobě dokumenty programů MS Office (Word, Excel, PowerPoint), které mohou obsahovat škodlivý kód. Je zakázáno stahovat spustitelné soubory z prostředí sítě Internet, otevírat je či ukládat spustitelné soubory ze zpráv elektronické pošty a otevírat zprávy elektronické pošty doručené z neznámých zdrojů. V případě podezření na výskyt škodlivého kódu, nebo při výskytu podezřelých zpráv elektronické pošty nahlaste bezpečnostní incident. I v případě napadení škodlivým kódem je nutné toto zjištění neprodleně hlásit jako bezpečnostní incident.

## Čl. 11 Bezpečnostní incident

1. Přes všechna ochranná opatření se mohou vyskytnout bezpečnostní incidenty. Včasné zahájení odborného řešení bezpečnostního incidentu může velmi významně ovlivnit jeho průběh a dopady pro Nemocnici.
2. V případě zjištění vzniku nebo podezření na vznik kybernetického bezpečnostního incidentu je nutné jej co nejdříve nahlásit na Service Desk.
3. Doplnit konkrétní instrukce pro hlášení a jeho náležitosti – viz pracovní postupy na Intranetu

# Příloha 3. Bezpečnostní opatření pro IT pracovníky

## Čl. 1 Úvodní ustanovení

1. Nad rámec Bezpečnostních opatření pro uživatele Nemocnice XXXXXXXXXX (dále jen Nemocnice) v rámci SŘBI stanovuje bezpečnostní pravidla pro IT pracovníky a externí IT specialisty vykonávající činnosti pro zajištění bezpečnosti informací a kontinuity činností Nemocnice.

## Čl. 2 Působnost

1. Působnost směrnice se vztahuje na všechny IT pracovníky a externí IT specialisty, kteří provozují či spravují informační systémy nebo jiné prostředky Nemocnice. IT pracovníci a externí IT specialisté povinni dodržovat mimo zásady níže uvedené rovněž všechny zásady platné pro běžné uživatele.

## Čl. 3 Bezpečnostní požadavky na provoz a správu IT technologií

1. Pro provoz informačních a komunikačních technologií jsou z pohledu bezpečnosti informací stanoveny nad rámec přílohy č. 2 Bezpečnostní opatření pro uživatele následující minimální bezpečnostní požadavky a pracovní zásady.

## Čl. 4 Klasifikace aktiv

1. Aktiva typu IT služby / systémy / aplikace, která zahrnují hardware, software a další prvky tvořící počítačové sítě Nemocnice. Primárním aktivem se rozumí informace nebo služby poskytované informačním systémem Nemocnice. Podpůrná aktiva zajišťují funkčnost resp. dostupnost primárních aktiv – např. programové vybavení, technické vybavení, komunikační prostředky, objekty, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému Nemocnice.
2. K aktivům musí být vedena evidence umožňující jejich jednoznačnou identifikaci, druh, popis, garanta (vlastníka) aktiva a aktuálního správce. Pro podpůrná aktiva je rovněž evidována vazba na odpovídající primární aktiva, tj. pomocí které IT služby / systému / aplikace se data ukládají a zpracovávají nebo kterou činnost či proces Nemocnice podporují.
3. Provoz IT stanovuje a realizuje technická opatření k zajištění bezpečnosti všech aktiv Nemocnice v rámci celého jejich životního cyklu.
4. Média (papírové dokumenty, externí HDD, CD/DVD/BR, paměťové karty, USB disky, pásky, paměť telefonů, …) obsahující klasifikované informace musí být před vyřazením bezpečně zlikvidovány a během převozu musí být chráněny proti neoprávněnému přístupu, zneužití, nežádoucí modifikaci nebo narušení.

## Čl. 5 Bezpečnostní povědomí

1. Požadavky na úvodní a pravidelná školení správců a pracovníků obsazených do bezpečnostních rolí stanovuje plán rozvoje bezpečnostního povědomí. Za plánování a realizaci školení odpovídá útvar HR.
2. Požadavky na odborné znalosti a praxi s konkrétními technologiemi provozovanými v rámci informačních systémů Nemocnice jsou součástí požadavků na uchazeče v rámci výběrového řízení. Nedisponuje-li vybraný uchazeč znalostmi a praxí se správou konkrétní technologie, před převzetím oprávnění správce k dané technologii musí být odpovídajícím způsobem zaškolen (výrobcem, servisním partnerem, kolegy, …). Způsob a požadavky na formu zaškolení stanovuje nadřízený pracovník. Minimální zásady pro vedoucí IT pracovníky odpovědné za informační bezpečnost obsahuje elearningový kurz kybernetické bezpečnosti s názvem Šéfuj kyber! poskytovaný NÚKIB.
3. Požadavky na pravidelná školení správců a pracovníků obsazených do bezpečnostních rolí musejí pokrývat nejen bezpečnostní trendy a obecné hrozby, jimž je prostředí Nemocnice vystaveno, ale také konkrétní produkty a technologie, které pracovníci spravují. Proškolení na příslušné technologie musí být provedeno nejpozději v okamžiku jejich začlenění do provozního prostředí Nemocnice. Průběžná školení správců a pracovníků obsazených do bezpečnostních rolí v oblasti bezpečnosti informací musejí být realizována opakovaně a to nejméně jedenkrát ročně.

## Čl. 6 Řízení přístupu

1. Každý uživatel, správce a aplikace přistupující k informačnímu systému nebo k jednotlivým IT technologiím musí mít přidělen jednoznačný identifikátor (identita - přihlašovací jméno - login).
2. Přístup k informačním systémům může být přidělen pouze oprávněným uživatelům. Každé přidělení či odebrání přístupu je dokumentováno a to i včetně dočasně udělených.
3. Přístupová oprávnění jsou uživatelům přidělována na základě předem definovaných a Garantem schválených přístupových vzorů dle pracovního zařazení.
4. Individuální přidělování práv uživatelům je možné pouze na základě schválené žádosti uživatele o rozšíření oprávnění.
5. Za nouzových situací je možné přidělit oprávnění potřebná k odvrácení krizového stavu či minimalizaci dopadu bez schválení ale pouze dočasně na dobu nezbytnou k řešení nouzové situace.
6. Přidělení privilegovaných oprávnění (práva správce) je možné pouze osobám pověřeným výkonem správy informačního systému či zařízení.
7. Přihlašovací hesla pro privilegované účty je nutné volit odolnější nežli uživatelské, tvorba hesel pro privilegované účty je uvedena níže.
8. Správci zajistí nastavení vyžadování následujících politik hesel u všech přímo spravovaných systémů i všech v systémech využívaných v rámci outsourcingu.
9. Pro použité systémové privilegované účty a účty pro systémové služby (vestavěný administrátorské účty k OS a DB, - Admin, root, SA, a pod) IT zajistí bezpečné uložení jejich kopií (vytištěné a uložen v bezpečnostní obálce v trezoru) a zavede jejich řízené používání za nouzových a kritických stavů.
10. Přidělené identity a přístupových oprávnění uživatelům jsou dokumentovány a spravovány v nástroji na řízení identit a přístupových práv.
11. Přidělení identit a přístupových oprávnění je dokumentováno a pravidelně přezkoumáváno automatizovanou/ruční kontrolou porovnávající stav schválených a skutečně zavedených identit a nastavených přístupových oprávnění v systémech, aplikacích a technologiích.
12. Nemocnice má zavedena organizační či technická opatření umožňující bezpečné používání mobilních zařízení (chytré telefony a tablety) pro přístup k interním informačním službám (mail, intranet, …).
13. Pro hesla správce do informačních systémů Nemocnice platí tyto požadavky:

|  |  |
| --- | --- |
| Minimální délka: | 17 znaků |
| Minimální platnost: | 30 minut |
| Komplexnost: | Heslo musí obsahovat minimálně 3 z těchto požadavků:  - jedno velké písmeno,  - jedno malé písmeno,  - jednu číslici,  - jeden speciální znak (. , - \* \_ + # $ apod.). |
| Povinná změna: | Minimálně 1x za 18 měsíců |
| Opakovatelnot: | Stejné heslo se nesmí opakovat min. 12 změn zpět. |

1. Politika pro účty systémových služeb:

|  |  |
| --- | --- |
| Minimální délka: | 32 znaků |
| Komplexnost: | Heslo musí obsahovat minimálně 3 z těchto požadavků:  - jedno velké písmeno,  - jedno malé písmeno,  - jednu číslici,  - jeden speciální znak (. , - \* \_ + # $ apod.). |
| Povinná změna: | Minimálně 1x za 18 měsíců, nevztahuje se na účty k obnově systému v případě havárie |
| Opakovatelnot: | Stejné heslo se nesmí opakovat min. 12 změn zpět. |

1. Doplnit konkrétní instrukce pro přidělení oprávnění – viz pracovní postupy IT na Intranetu
2. Doplnit konkrétní instrukce pro změnu oprávnění – viz pracovní postupy IT na Intranetu
3. Doplnit konkrétní instrukce pro odebrání oprávnění – viz pracovní postupy IT na Intranetu
4. Doplnit konkrétní instrukce pro kontroly oprávnění – viz pracovní postupy IT na Intranetu

## Čl. 7 Kryptografická ochrana

1. Pro zajištění důvěrnosti a integrity informací musí být uživatelům dostupné adekvátní kryptografické prostředky. Pro účinné zajištění ochrany informací musí být k danému účelu použity pouze dostatečně odolné kryptografické algoritmy splňující minimální požadavky uvedené v příloze 1 tohoto dokumentu.
2. Pro použití kryptografických prostředků musí být zaveden systém správy klíčů a zajištěna jejich adekvátní ochrana.
3. Doplnit konkrétní instrukce pro systém správy klíčů a certifikátů – viz pracovní postupy IT na Intranetu
4. Doplnit konkrétní SW a instrukce k nastavení vzdáleného přístupu pomocí VPN – viz pracovní postupy IT na Intranetu
5. Doplnit konkrétní SW a instrukce k nastavení šifrování souborů – viz pracovní postupy IT na Intranetu
6. Doplnit konkrétní SW a instrukce k nastavení elektronického podpisu – viz pracovní postupy IT na Intranetu

## Čl. 8 Fyzická bezpečnost

1. Fyzická bezpečnost objektů, místností, kabelových tras a řízení vstupů rovněž jako dodávka napájení včetně záložních zdrojů a provoz klimatizace je zajišťováno útvarem FM. Standardy a postupy pro tuto oblast jsou stanoveny v rámci politiky fyzické bezpečnosti.
2. Výpočetní technika je umístěna v objektech Nemocnice. Před neoprávněnými osobami je zabezpečena uzamčením (v místnosti, heslem, pinem, atp.) či dohledem pracovníků Nemocnice.
3. V rámci fyzického zabezpečení technologií IT zajišťuje informační technologie a používaná datová média před jejich zcizením, zničením a přístupem neoprávněných osob jejich umisťováním do určených prostor (datové centrum, místnost pro servery, místnost pro rozvaděče, …). Servisní zásahy pracovníků třetích stran jsou vykonávány řízeně a pod dohledem IT provozu.
4. Útvar IT zajišťuje údržbu HW a SW jako prevenci proti jejich výpadku a ztrátě integrity (narušení). Přemisťování HW a SW nesmí být prováděno bez předchozího schválení oprávněnou osobou.
5. IT technologie a media umístěná mimo organizaci (během přepravy, uložení záloh, …) musí být chráněna adekvátně k jejich hodnotě a hodnotě informačních aktiv na nich umístěná. Ochranná opatření musí pokrývat i rizika působící v prostředí mimo Nemocnici.
6. Útvar IT definuje organizační (procesní) a technologické postupy pro opětovné použití a vyřazení zařízení a médií (PC, notebooky, servery, HDD, paměťové karty, USB disky, pásky, paměť telefonů, …) tak, aby byla zajištěna bezpečná likvidace klasifikovaných informací v zařízeních a médiích obsažených.
7. Útvar IT aplikuje opatření k zabezpečení neobsluhovaných zařízení:

• uzamčení PC a serverů při nečinnosti delší než 15/30/… minut,

• ukončení aktivních spojení k informačním systémům při nečinnosti delší než 15/30/… minut.

tak, aby uživatel byl nucen se znovu autorizovat (zadat heslo či přístupový kód) pro další použití zařízení či informačního systému.

1. Doplnit konkrétní instrukce dle specifik areálu či objektu – viz pracovní postupy IT na Intranetu

## Čl. 9 Provoz a komunikace

1. Útvar IT pro Nemocnici provozuje informační a síťové technologie a navrhuje infrastrukturu a topologii sítě. Zajištuje bezpečnosti informací, ukládaných, zpracovávaných a přenášených prostřednictvím informačních systémů a sítí.
2. Za tímto účelem útvar IT zavede, provozuje a pravidelně vyhodnocuje nástroj pro zaznamenávání činnosti informačních systémů, aplikací a prvků sítě, jejich uživatelů a správců (provozní monitoring) a nástroj pro sběr a vyhodnocování kybernetických bezpečnostních událostí (bezpečnostní monitoring).
3. Útvar IT k podpoře bezpečnosti provozu a komunikací SŘBI zavádí pravidla, postupy, stanoví odpovědnosti a implementuje technická opatření pro zajištění:

• vedení dokumentovaných provozních postupů,

• řízení změn,

• řízení kapacit,

• uplatnění principu oddělení prostředí vývoje, testování a provozu,

• opatření na ochranu proti škodlivému kódu,

• pravidla a technické prostředky pro zálohování informací,

• monitoring a zaznamenávání provozních událostí formou logů,

• pravidla a technické prostředky k ochraně provozních logů,

• zaznamenávání událostí (logy) o činnosti administrátorů a uživatelů,

• synchronizaci hodin na informačních systémech a síťových zařízeních,

• správy a řízené instalace softwaru na provozní systémy,

• detekci a řízení technických zranitelností,

• omezení instalace neprověřeného softwaru,

• na poskytnutí součinnosti k auditu IT (technické testy konfigurace, penetrační testování, …) při zachování minimalizace dopadů na informační systémy a síťové prvky,

• bezpečnostní koncepce a opatření v sítích,

• bezpečnost síťových služeb,

• princip oddělení v sítích,

• politiky a postupy pro přenos informací,

• přenos informací se třetími stranami (požadavky do smluv),

• elektronické předávání zpráv (email, sociální sítě, …),

• dohody o mlčenlivosti.

1. Doplnit konkrétní instrukce pro jednotlivá opatření – viz pracovní postupy IT na Intranetu

## Čl. 10 Dodavatelé

1. Útvar IT stanoví pravidla pro dodavatele na realizaci dodávky HW, SW, implementačních projektů nových a rozvojových projektů, podporu a údržbu stávajících IT technologií. Kontroluje, že se tato pravidla stávají povinnou součástí smluv s dodavateli.
2. Útvar IT ve smlouvě s dodavatelem prokazatelně dokumentuje rozsah jeho zapojení včetně subdodavatelů na rozvoji, provozu či zajištění bezpečnosti informačního systému Nemocnice.
3. Útvar IT kontroluje, že součástí smluv s dodavateli je taktéž ujednání o ochraně informací a adekvátní smlouva o zachování mlčenlivosti (NDA).
4. Útvar IT v zadání požadavků do smluv aplikuje výstupy a doporučení vyplývající z provedené analýzy rizik a stanovuje potřebná bezpečnostní opatření, způsoby a úrovně realizace bezpečnostních opatření a určí vztah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.
5. Útvar IT zajišťuje pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u služeb dodavatelů a zajišťuje odstranění zjištěných nedostatků.
6. K naplnění výše uvedených požadavků útvar IT prosazuje přenesení smluvních povinností na celý dodavatelský řetězec. Provádí:

• monitorování a přezkoumání služeb dodavatelů,

• řízení změn ve službách dodavatelů.

## Čl. 11 Kontinuita činností

1. Útvar IT plánuje a realizuje opatření k zajištění dostupnosti informačních a komunikačních technologií minimálně na úrovni BCM parametrů definovaných výstupy analýzy rizik a dopadů a schválených pracovníky odpovědnými za zachování kontinuity činností Nemocnice.
2. Útvar IT na základě definovaných požadavků a výstupů analýzy rizik a dopadů definuje strategii obnovy IT služeb, připravuje plány obnovy jednotlivých systémů (DRP) a prověřuje jejich funkčnost a efektivitu. Definuje a pravidelně prověřuje plán obnovy procesů IT nezbytných k zajištění dodávky IT služeb Nemocnice. O provedených testech vede záznam a zjištěné nedostatky plánů obnovy neprodleně odstraňuje.
3. Technickými opatřeními útvar IT zajišťuje požadovanou dostupnost informačních systémů Nemocnice.

## Čl. 12 Soulad s požadavky

1. Útvar IT zajišťuje dílčí kontroly souladu aplikovaných technických bezpečnostních opatření s definovanými provozními standardy a bezpečnostními požadavky.
2. Rovněž monitoruje dodržování smluvních SLA dodavateli a u zjištěných nedostatků přijímá opatření k nápravě, popřípadě iniciuje uplatnění smluvních sankcí.
3. Z dílčích kontrol útvar IT provádí zejména:

• kontrolu souladu schválených a skutečně nastavených přístupových oprávnění uživatelů v informačních systémech a síťových prvcích,

• kontrolu dodržování licenčních práv používaného SW,

• kontrolu souladu kryptografických opatření s legislativní regulací a upravuje kryptografické standardy,

• kontrolu zranitelností informačních systémů, aplikací a síťových prvků pomocí automatizovaných nástrojů, zjištěné zranitelnosti odborně vyhodnocuje a aplikuje potřebná opatření k jejich snížení nebo odstranění.

1. O vykonaných kontrolách vede útvar IT záznamy, které zajišťuje před jejich ztrátou, únikem či nežádoucí modifikací.

# Příloha 4. Přechodná ustanovení

## Čl. 1 Úvodní ustanovení

1. Nemocnice XXXXXXXXXX (dále jen Nemocnice) s ohledem na ochranu investic, platný plán investic a aktuální technické možnosti informačního systému Nemocnice stanovuje pro konkrétní ustanovení politiky následující přechodné období, kdy budou v cílovém stavu plně prosazena.

## Čl. 2 Působnost článku politiky či ustanovení

1. Vymezit konkrétní článek/bod/ustanovení pro daný informační systém Nemocnice.

# Příloha 5. Přehled související legislativy

Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)

Vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci

Zákon č. 373/2011 Sb., o specifických zdravotních službách

Zákon č. 374/2011 Sb., o zdravotnické záchranné službě

Zákon č. 48/1997 Sb., o veřejném zdravotním pojištění

Zákon č. 378/2007 Sb., o léčivech

Zákon č. 268/2014 Sb., o diagnostických zdravotnických prostředcích in vitro

Zákon č. 258/2000 Sb., o ochraně veřejného zdraví

Zákon č. 285/2002 Sb., o darování, odběrech a transplantacích tkání a orgánů (transplantační zákon)

Zákon č. 296/2008 Sb., o lidských tkáních a buňkách

Zákon č. 110/2019 Sb., o zpracování osobních údajů

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby

Nařízení Evropského parlamentu a Rady (EU) 2016/679 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

Zákon č. 110/2019 Sb., o zpracování osobních údajů

Sdělení č. 115/2001 Sb. m. s., Ministerstva zahraničních věcí o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat