



S-KB-002

Bezpečnostní politiky Nemocnice Strakonice, a.s.

1. vydání

1 ZÁKLADNÍ PRINCIPY

Péče o pacienty a provoz zdravotnických služeb jsou zcela závislé na efektivním sběru a zpracování údajů o pacientech, zaměstnancích a dalších spolupracujících subjektech. Za ochranu těchto informací nese odpovědnost každý zaměstnanec organizace.

Naším primárním cílem je zajistit bezpečnost informačního majetku organizace.

Zásada ochrany soukromí

Zachování důvěrnosti údajů – ať už se jedná o zdravotní informace pacientů či osobní data zaměstnanců a partnerů – je základem ochrany soukromí. Integrita dat spočívá především v respektování mlčenlivosti a v dodržování bezpečných komunikačních zásad – ať už jde o verbální, písemnou nebo elektronickou formu.

Zásada dostupnosti

Dostupnost informací je klíčovým faktorem při poskytování kvalitní péče. Usilujeme o vysoký standard přístupnosti dat, přičemž důraz klademe na bezpečnost sdílení informací.

Zásada bezpečnosti

Zdravotnické informační systémy čelí rizikům jak z vnějších zdrojů (např. kybernetické útoky), tak i z vnitřního prostředí. Důkladně nastavujeme bezpečnostní mechanismy s cílem minimalizovat potenciální hrozby. Informace chráníme po celou dobu jejich životního cyklu – od získání přes zpracování, uložení a přenos až po výstup. Každý dodavatel, jenž se podílí na ICT infrastruktuře nebo má přístup k našim datům, musí splňovat přísné bezpečnostní požadavky.

Zásada ochrany

Zajišťujeme ochranu klíčových procesů před narušením, zcizením nebo zneužitím. Řídíme přístup k informacím, kontrolujeme fyzický vstup do chráněných prostor a uplatňujeme bezpečnostní opatření pro přenosná zařízení a datové nosiče. Dodavatelé s přístupem k našemu majetku jsou rovněž vázáni příslušnými pravidly.

Zásada prevence

Systematicky identifikujeme a vyhodnocujeme potenciální rizika. Vycházíme z výsledků analýz a auditů, které nám pomáhají vytvářet preventivní strategie. Na prvním místě je pro nás eliminace hrozeb s vysokým dopadem na celkovou bezpečnost systému. Soustavně sledujeme, hodnotíme a přezkoumáváme výkonnost dodavatelů.

Zásada uvědomění

Každý uživatel systému musí rozumět hrozbám, které se k oblasti bezpečnosti pojí, a být připraven aktivně dodržovat bezpečnostní politiku. Zaměstnanci vykonávající role v oblasti bezpečnosti procházejí odborným vzděláváním. Politika bezpečnosti informací je závazná pro všechny, kdo mají přístup k citlivým datům, bez ohledu na pozici. Stejná pravidla platí i pro dodavatele, s nimiž jsou podmínky bezpečnosti smluvně upraveny. Porušení pravidel je považováno za bezpečnostní incident s odpovídajícími důsledky.

Zásada praxe

Bezpečnostní standardy nejsou jen teoretickými pravidly – jsou systematicky uváděny do každodenní praxe. Udržování bezpečnostních opatření je neustálý, kontinuální proces.

Zásada zdrojů

Vytváříme organizační a ekonomické podmínky pro účinné zavedení, správu i další rozvoj systému bezpečnosti informací. Náklady spojené se zajištěním bezpečnosti jsou plánovány s ohledem na hodnotu chráněných dat a efektivitu vynaložených prostředků.

Zásada rozvoje

Sledujeme aktuální technologické trendy a podle nich přizpůsobujeme ochranu našich informačních aktiv. Zálohujeme systémy, chráníme data dle platné legislativy a usilujeme o neustálé zlepšování procesů souvisejících s ochranou informací.

Zásada kontinuity

Bezpečnostní politika není statickým dokumentem. Průběžně ji aktualizujeme s ohledem na změny vnitřního i vnějšího prostředí a nové legislativní požadavky.

Zásada ochrany soukromí pacientů, návštěvníků a zaměstnanců

Pořizování jakýchkoliv záznamů v prostorách nemocnice se řídí platnými právními předpisy:

V prostorách nemocnice je zakázáno pořizovat obrazové či zvukové záznamy, pokud na nich mají být zachyceny osoby bez jejich výslovného souhlasu. Výjimku tvoří média se zpravodajskou licenci, pokud je záznam pořízen výhradně pro účely informování veřejnosti.

Natáčení v porodnici je přípustné pouze se souhlasem primáře a výhradně za situace, kdy se záznam týká matky, dítěte a přítomného otce. Jeho účel musí být čistě rodinný a dokumentační.

Výjimky z těchto pravidel může nemocnice povolit na základě odůvodněné žádosti podané bezpečnostnímu a krizovému manažerovi.

Zástupci médií jsou povinni o záměru pořizovat záznamy předem informovat vedení nemocnice nebo tiskového mluvčího – telefonicky (kontakty jsou uvedeny na webových stránkách) nebo písemně prostřednictvím e-mailu.

2 POLITIKA ŘÍZENÍ PROVOZU A KOMUNIKACÍ

2.1 PŘEDMĚT

Účelem této Politiky řízení provozu a komunikací je zajistit spolehlivý, stabilní a bezpečný provoz IS a podpůrných aktiv tak, aby byla zaručena bezpečnost primárních aktiv.

2.2 PRAVOMOCI A ODPOVĚDNOSTI SPOJENÉ S BEZPEČNÝM PROVOZEM

1. Provozovatel IS v rámci řízení provozu a komunikací pomocí technických nástrojů pro zaznamenávání činností IS, jejich uživatelů a administrátorů pravidelně vyhodnocuje získané informace a na zjištěné nedostatky reaguje v souladu s postupy zvládnání bezpečnostních událostí a incidentů (BU a BI).
2. Provozovatel IS v rámci řízení provozu a komunikací zajišťuje bezpečný provoz IS. Za tímto účelem stanoví pravidla a postupy v provozní dokumentaci a bezpečnostní dokumentaci.

2.3 POSTUPY BEZPEČNÉHO PROVOZU

1. Provozní postupy IS jsou dokumentovány v provozní dokumentaci. Za vedení provozní dokumentace odpovídá příslušný garant aktiva a administrátor.
2. Bezpečnostní postupy IS jsou dokumentovány v bezpečnostní dokumentaci. Za vedení bezpečnostní dokumentace odpovídá příslušný správce informačních technologií.
3. Postupy bezpečného provozu zahrnují zejména:
 - a) práva a povinnosti osob zastávajících role zejména administrátorů a uživatelů,
 - b) postupy pro spuštění a ukončení chodu IS, pro restart nebo obnovení chodu IS po selhání a pro ošetření chybových stavů nebo mimořádných jevů,
 - c) postupy pro sledování BU a BI a pro ochranu přístupu k záznamům o těchto činnostech,
 - d) kontaktní údaje na osoby, které jsou určeny jako podpora při řešení neočekávaných systémových nebo technických problémů,
 - e) postupy řízení a schvalování provozních změn.
4. Provozní dokumentaci tvoří zejména:
 - a) provozní deník,
 - b) plán kontrol řízení provozu,
 - c) evidence kontrol řízení provozu,
 - d) zálohovací plán, komunikační matice pro případ vzniku neočekávaných provozních nebo technických problémů,
 - e) speciální instrukce pro zacházení s výstupy a médii,
 - f) procedury pro restart a obnovu v případě selhání IS.
 - g) požadavky a standardy bezpečného provozu

2.4 ŘÍZENÍ ZMĚN

1. Veškeré změny v organizaci, provozních procesech, informačních systémech a ve vybavení pro zpracování informací, které mohou mít vliv na bezpečnost informací, musí být dokumentovány.
2. Dokumentace musí obsahovat informace o tom, kdo je oprávněn provádět změny. Změny pak mohou provádět pouze osoby k tomu oprávněné.
3. Musí existovat formální procesy pro řízení změn informačních systémů Nemocnice Strakonice, a.s., které zahrnují:
 - a) způsob identifikace a zaznamenání významných změn,
 - b) plánování a testování změn,
 - c) posouzení možných dopadů těchto změn a ověření, zda byly splněny požadavky na bezpečnost informací,
 - d) formální postup schvalování navrhovaných změn a seznámení všech příslušných osob s podrobnostmi změn,
 - e) postupy pro přerušování prováděných změn a obnovení provozu po implementaci neúspěšných změn a při nepředvídaných událostech.

2.5 ŘÍZENÍ KAPACIT

1. Řízení kapacit je založeno na stanovení kapacitních nároků pro každý IS. Provozovatel IS odpovídá za celkové sledování kapacit, předpokládaný vývoj a návrh případných nápravných opatření.
2. Prvky podléhající řízení kapacit jsou:
 - a) hardware (výkon, licence)
 - b) software (verze, licence),
 - c) komunikační infrastruktura (propustnost),
 - d) pracovní prostory (prostory pro hardware včetně vybavení, kancelářské prostory),
 - e) personální obsazení.

V případě zjištění kapacitního nedostatku musí být tato skutečnost sdělena garantovi systému, případně příslušnému vedení.

2.6 ODDĚLENÍ PROSTŘEDÍ VÝVOJE, TESTOVÁNÍ A PROVOZU

Vývojové a testovací prostředí musí být odděleno od provozního prostředí. V provozním prostředí nesmí být dostupné nástroje pro vývoj, jako jsou například kompilátory. Provozní a projektová dokumentace stanoví, za jakých podmínek dochází k přesunu systému z fáze vývoje a testování do provozního stavu.

2.7 ZAZNAMENÁVÁNÍ UDÁLOSTÍ

1. Musí být automaticky vytvářeny záznamy událostí obsahující aktivity uživatelů, výjimky a závady v provozu systémů a dále události bezpečnosti informací.
2. Tyto záznamy musí být uchovávány po dobu minimálně 12 měsíců. Záznamy musí být pravidelně přezkoumávány.
3. Zaznamenané logy musí obsahovat minimálně tyto informace:
 - a) jednoznačnou identifikaci účtu (procesu), pod kterým byla činnost provedena,
 - b) datum a čas události,
 - c) identifikaci zařízení (technického aktiva), které činnost zaznamenalo,
 - d) informace o typu činnosti.
4. Dále musí logy obsahovat tyto informace, jsou-li relevantní pro danou činnost:
 - a) záznamy o úspěšných a odmítnutých pokusech o přístup k systému nebo informacím;
 - b) změny konfigurace systému,
 - c) soubory, ke kterým bylo přistupováno,
 - d) jednoznačnou síťovou identifikaci zařízení, včetně použitých protokolů,
 - e) úspěšnost nebo neúspěšnost činnosti,
 - f) záznamy transakcí provedených uživateli.

Musí být zamezeno pokusům o neoprávněný přístup k logům, jejich neautorizovanou změnu nebo vymazání.

2.8 PRAVIDLA A OMEZENÍ PRO PROVÁDĚNÍ AUDITŮ KYBERNETICKÉ BEZPEČNOSTI A BEZPEČNOSTNÍCH TESTŮ

1. Audit KB a bezpečnostní test nesmí omezit provoz a bezpečnost auditovaných IS.
2. Audit KB za účelem ověření provozu IS je naplánován tak, aby se minimalizovalo narušení činnosti auditovaného subjektu.
3. V případě, že Auditor KB potřebuje jiný typ přístupu než pouze pro čtení, vyhotoví provozovatel IS kopie požadovaných souborů a předá je Auditorovi KB. Kopie souborů se po ukončení auditu auditorem smazají nebo, pokud je to vyžadováno Auditorem KB pro dokumentaci auditu, musí být řádným způsobem chráněny.
4. Požadavky, postupy a odpovědnosti Auditora KB jsou dokumentovány.
5. Přístupy Auditora KB jsou monitorovány a logovány.

3 POLITIKA ŘÍZENÍ PŘÍSTUPU

3.1 PŘEDMĚT

Účelem této části Politiky řízení přístupu je:

- a) definovat princip a stanovit minimální oprávnění,
- b) definovat požadavky na nastavení přístupových práv pro uživatele, privilegované uživatele a bezpečnostní role včetně souvisejících procesů,
- c) stanovit fáze řízení přístupových práv,
- d) definovat základní požadavky na technologické účty,
- e) specifikovat základní principy pro privilegovaná oprávnění a omezení při jejich užití,
- f) specifikovat proces pro přidělování, správu a rušení přístupových práv v případě mimořádných situací,
- g) určit způsob a četnost kontrol přístupových práv.

3.2 PRAVIDLA A POŽADAVKY NA ŘÍZENÍ PŘÍSTUPU

1. Za řízení přístupu a stanovení pravidel je odpovědný garant příslušného aktiva.
2. Za stanovení pravidel v oblasti řízení přístupu je odpovědný provozovatel IS.
3. Musí existovat evidence všech uživatelských účtů, pomocí které je možné jednoznačně identifikovat osobu používající daný uživatelský účet.
4. Přístupy a pokusy o přístup musí být automaticky zaznamenávány a monitorovány. Záznamy musí být uchovány po dobu minimálně 18 měsíců u systémů provozovaných jako kritická informační infrastruktura a po dobu minimálně 12 měsíců u ostatních systémů. U uživatelských účtů musí být nastaveno automatické uzamčení obrazovky při nepřítomnosti uživatele. Pro opětovné odemčení musí být vyžadovány autentizační údaje.
5. Autentizační údaje nesmí být sdíleny více osobami.
6. Přidělování přístupových práv se řídí pravidly:
 - a) každý prvek ICT má řízený a dokumentovaný proces přidělování přístupových práv,
 - b) je prováděna pravidelná kontrola řízení přístupových práv a stanovených pravidel pro řízení přístupových práv,
 - c) přidělování přístupových práv uživatelům je prováděno pouze v rozsahu nutném pro výkon jejich služebních, resp. pracovních povinností,
 - d) kontrola přidělených přístupových práv je prováděna při každé změně a minimálně jednou za rok,
 - e) pro každý prvek ICT je vedena aktuální evidence všech uživatelských účtů,
 - f) pro každý prvek ICT je definován systém uživatelských rolí a oprávnění,
 - g) je vedena evidence o uskutečněných přístupech a o pokusech o přístup k aktivu,
 - h) primárním nástrojem pro řízení uživatelů je nástroj Identity management (IDM)
 - i) zákaz přístupu k aktivům prostřednictvím veřejných sítí např. z nechráněné sítě v restauracích apod.,
 - j) je využívána vícefaktorová autentizace,
 - k) role uživatelů, privilegovaných uživatelů a bezpečnostních rolí jsou odděleny,
 - l) postup řízení přístupů při mimořádných situacích je dokumentován.

3.3 PRINCIP MINIMÁLNÍCH OPRÁVNĚNÍ A POTŘEBY ZNÁT (NEED TO KNOW)

Pravidla pro řízení přístupových oprávnění:

- a) Každý uživatel má přístup pouze k těm aktivům, která nezbytně potřebuje k výkonu práce.
- b) Základní rozsah oprávnění k jednotlivým aktivům je definován jako minimum potřebného pro činnosti, které uživatel potřebuje. Oprávnění jsou členěna do uživatelských rolí.
- c) Změna rozsahu přístupových oprávnění je řízena a schvalována.

3.4 MINIMÁLNÍ POŽADAVKY NA SYSTÉM ŘÍZENÍ PŘÍSTUPU

Systém řízení přístupu je tvořen minimálně:

- a) popisem rozsahu jednotlivých uživatelských rolí,
- b) popisem požadavku na školení jednotlivých uživatelských rolí,
- c) definicí kritické kombinace rolí,
- d) popisem procesu přidělování uživatelských rolí,
- e) popisem technologie ověření identity uživatelů,
- f) popisem bezpečného chování uživatelů,
- g) definicí životního cyklu přístupových údajů uživatelů,
- h) vynucováním pravidel pro ověření identity uživatelů.

3.5 ŽIVOTNÍ CYKLUS ŘÍZENÍ PŘÍSTUPU

1. Řízení přístupu je dokumentováno pro každé aktivum a probíhá ve fázích:
 - a) žádost o přidělení přístupových práv,
 - b) schvalování a přidělení přístupových práv,
 - c) pravidelná kontrola přístupových práv,
 - d) změna přístupových práv,

- e) zrušení přístupových práv.
2. V žádosti o přidělení přístupových práv jsou definovány minimálně:
 - a) osoba oprávněna žádat,
 - b) uživatel,
 - c) rozsah oprávnění a jejich zdůvodnění,
 - d) doba platnosti oprávnění.
 3. V procesu schvalování a přidělení přístupových práv je definován minimálně:
 - a) osoby oprávněné schválit požadavek,
 - b) schvalovací lhůty,
 - c) osoby nastavující příslušná oprávnění.
 4. V procesu změny přístupových práv je definována minimálně:
 - a) osoba oprávněna žádat,
 - b) uživatel,
 - c) požadavek na změnu rozsahu oprávnění,
 - d) doba platnosti oprávnění,
 - e) osoby oprávněné schválit požadavek,
 - f) schvalovací lhůty,
 - g) osoby nastavující příslušná oprávnění.
 5. Ke zrušení přístupových práv k informacím a aktivům dochází:
 - a) při ukončení nebo změně pracovního nebo smluvního vztahu nebo výkonu role uživatele,
 - b) na základě procesů definovaných v provozní dokumentaci jednotlivého aktiva.

3.6 ŘÍZENÍ PRIVILEGOVANÝCH OPRÁVNĚNÍ

1. Privilegovaným oprávněním se rozumí přístupové oprávnění k účtu, které umožňuje v jednotlivém prvku ICT:
 - a) vykonávat činnosti nad rámec běžného uživatele IS,
 - b) provádět změny v nastavení IS,
 - c) měnit rozsah přidělených oprávnění jednotlivých rolí a uživatelů,
 - d) vykonávat servisní činnosti bez přítomnosti uživatele.
2. Pro privilegované oprávnění je přiřazen odlišný identifikátor uživatele od běžně používaného uživatelského účtu.
3. Běžné činnosti nesmějí být prováděny s použitím privilegovaného oprávnění.
4. Musí být nastaveno časové omezení platnosti přihlašovací relace, po jehož vypršení následuje automatické odhlášení od systému.

3.7 ŘÍZENÍ PŘÍSTUPU PRO MIMOŘÁDNÉ SITUACE

1. Za účelem zajištění kontinuity činnosti během BU, BI nebo jiných mimořádných situací jsou jednorázově nastavena přístupová oprávnění nad rámec standardního režimu provozu prvku ICT.
2. Procesy pro zvládnutí BU, BI nebo jiné mimořádné situace jsou definovány v havarijním plánu a zpracované pro všechna relevantní informační aktiva.

3.8 PRAVIDELNÉ PŘEZKOUMÁNÍ PŘÍSTUPOVÝCH OPRÁVNĚNÍ

1. Proces pro přezkoumání přístupových oprávnění je definován v bezpečnostní dokumentaci zpracované pro každé aktivum.
2. Kontrola přístupových oprávnění v jednom cyklu je provedena na celém rozsahu uživatelských oprávnění.
3. Dokumentace pro přezkoumání přístupových oprávnění obsahuje minimálně:
 - a) stanovení cyklu provádění kontroly,

- b) osoby provádějící kontrolu,
- c) zápis o provedené kontrole,
- d) postup nápravy při zjištění nedostatku.

4 POLITIKA BEZPEČNÉHO PŘEDÁVÁNÍ A VÝMĚNY INFORMACÍ

4.1 PŘEDMĚT

Účelem této části Politiky bezpečného předávání a výměny informací je stanovit pravidla a způsob ochrany pro předávání informací a definovat:

- a) Pravidla a postupy pro ochranu předávaných informací
- b) Způsoby ochrany elektronické výměny informací
- c) Pravidla pro využívání kryptografické ochrany

4.2 PRAVIDLA A POSTUPY PRO OCHRANU PŘEDÁVANÝCH INFORMACÍ

1. K ochraně přenosu informací prostřednictvím všech druhů komunikačních zařízení jsou stanoveny postupy a opatření na základě klasifikace informací.
2. Dochází-li k předávání informací s externím subjektem (např. smluvní strana), podrobnosti o bezpečném předávání informací jsou definovány dohodou o předávání informací.
3. Dohoda o předávání informací obsahuje zejména:
 - a) rozsah předávaných informací,
 - b) způsob zabezpečení předávaných informací, včetně ochrany důvěrnosti, dostupnosti a integrity
 - c) účel užití předávaných informací,
 - d) technické parametry předávaných informací,
 - e) odpovědnosti a povinnosti v případě vzniku BU a BI,
 - f) dohodu o mlčenlivosti.
4. Za uzavření dohody o předávání informací odpovídá Garant příslušného aktiva, jehož aktivum je se smluvní stranou sdíleno.
5. Pro předávání informací je zakázáno využívat veřejná internetová úložiště (např. Google drive, One drive, DropBox apod.).
6. Uveřejňování informací na internetových stránkách www.nemst.cz je řízeno.

4.3 ZPŮSOBY OCHRANY ELEKTRONICKÉ VÝMĚNY INFORMACÍ

1. Během výměny informací musí být vhodným způsobem chráněny elektronicky přenášené informace.
2. Předávání informací, které jsou klasifikovány kategorií „citlivé“, pomocí elektronické pošty je podmíněno jejich zašifrováním. Za šifrování předávaných informací je odpovědný jejich odesílatel. Uživatelé nejsou oprávněni sdílet informace klasifikované kategorií „citlivé“ s externí stranou bez souhlasu jejich vlastníka.
3. Předávání informací, které jsou klasifikovány v kategorii „citlivé“, pomocí elektronické pošty, která při předání využije prostředky mimo přímou kontrolu společnosti (např. Microsoft Exchange), je podmíněno jejich zašifrováním.

4.4 PRAVIDLA PRO VYUŽÍVÁNÍ KRYPTOGRAFICKÉ OCHRANY

1. Kryptografická opatření jsou používána v případech nutnosti zajistit důvěrnost, dostupnost a integritu přenášených informací v souladu s klasifikací aktiv podle „Politiky řízení aktiv“
2. Používání prostředků kryptografické ochrany se řídí podle „Politiky používání kryptografické ochrany“.

5 POLITIKA BEZPEČNÉHO UŽÍVÁNÍ MOBILNÍCH ZAŘÍZENÍ

5.1 PŘEDMĚT

Tato politika bezpečného používání mobilních zařízení definuje:

- a) Pravidla a postupy pro bezpečné používání mobilních zařízení.
- b) Pravidla a postupy pro zajištění bezpečnosti zařízení, která povinná osoba nemá ve své správě.

5.2 PRINCIPY PRÁCE S MOBILNÍMI ZAŘÍZENÍMI

Politika práce s mobilními zařízeními je založena na následujících principech:

- a) Při použití mobilních výpočetních prostředků, například notebooků, laptopů a mobilních telefonů, musí být věnována zvláštní pozornost tomu, aby nebyly vyzrazeny informace Nemocnice Strakonice, a.s. Uživatel musí podle situace přijmout takové opatření, aby znemožnil zneužití informací společnosti.
- b) Pozornost musí být věnována použití mobilních výpočetních zařízení na veřejných místech, v zasedacích místnostech a jiných nechráněných místech mimo prostor Nemocnice Strakonice, a.s. Při použití zařízení na veřejných místech se uživatelé musí vyhnout riziku odpozorování neautorizovanými osobami. Měly by být použity prostředky proti škodlivým programům a tyto prostředky by měly být aktualizovány.
- c) Mobilní výpočetní prostředky musí být také chráněny proti zcizení, zejména pokud zůstávají například v autech nebo jiných dopravních prostředcích, hotelových pokojích, konferenčních centrech a zasedacích místnostech. V případě krádeže nebo ztráty mobilních výpočetních zařízení musí být tato skutečnost bez prodlení nahlášena nadřízenému pracovníkovi a Manažerovi KB. Ti zajistí další postup ve spolupráci se správcem IT organizace.

5.3 MOBILNÍ ZAŘÍZENÍ

Mobilními zařízeními se rozumí veškerá mobilní zařízení umožňující zobrazovat, editovat, ukládat, přenášet nebo tisknout data, tedy zejména:

- a) notebooky,
- b) tablety a podobná přenosná zařízení,
- c) telefony,
- d) vyjímatelné disky a paměťové karty používané na těchto zařízeních,
- e) flash paměti, digitální fotoaparáty, MP3 přehrávače apod.

5.4 PRAVIDLA BEZPEČNOSTI VE VZTAHU K MOBILNÍM ZAŘÍZENÍM

5.4.1 Pravidla a postupy pro bezpečné používání mobilních zařízení.

- a) Uživatel je povinen pro pracovní účely používat pouze ta mobilní zařízení, která mu byla přidělena.
- b) Provádění vlastní modifikace a instalace aplikací na mobilním zařízení je zakázáno.
- c) Uživatel je povinen chránit mobilní zařízení před krádeží a zneužitím.
- d) Uživatel je povinen bezodkladně hlásit ztrátu mobilního zařízení.
- e) Uživatel nesmí umožnit přístup do mobilního zařízení jiné osobě.
- f) Uživatel je povinen ve stanovených intervalech připojit mobilní zařízení do sítě společnosti za účelem provedení aktualizací a kontrol.
- g) Uživatel nesmí měnit nastavená bezpečnostní pravidla na zařízení.
- h) Uživatel je povinen chránit přístup do zařízení heslem, PINem, gestem nebo biometrickým prvkem.

5.4.2 Pravidla a postupy pro zajištění bezpečnosti zařízení, která povinná osoba nemá ve své správě.

- a) Uživatel je povinen pro pracovní účely používat odpovídající mobilní zařízení, která jsou schválena společností.
- b) Instalace aplikací na mobilním zařízení nesmí ohrozit informace zaměstnavatele.
- c) Uživatel je povinen chránit mobilní zařízení před krádeží a zneužitím.

- d) Uživatel je povinen bezodkladně hlásit ztrátu mobilního zařízení obsahující informace zaměstnavatele.
- e) Uživatel nesmí umožnit přístup k informacím zaměstnavatele v mobilním zařízení jiné osobě.
- f) Uživatel je povinen používat odpovídající bezpečnostní pravidla na zařízení.
- g) Uživatel je povinen chránit přístup do zařízení heslem, PINem, gestem nebo biometrickým prvkem.

5.5 NASTAVENÍ ZAŘÍZENÍ A KONTROLY

Za způsob nastavení mobilních zařízení odpovídá vedoucí IT, který definuje odpovídající postupy a kontroly v samostatném pracovním postupu.

6 POLITIKA BEZPEČNOSTI KOMUNIKAČNÍ SÍŤE

6.1 PŘEDMĚT

Účelem této Politiky bezpečnosti komunikační sítě je stanovit způsob ochrany komunikačních sítí Nemocnice Strakonice, a.s. tím, že definuje:

- a) Pravidla a postupy pro zajištění bezpečnosti sítě
- b) Určení práv a povinností za bezpečný provoz sítě
- c) Pravidla a postupy pro řízení přístupů v rámci sítě
- d) Pravidla a postupy pro ochranu vzdáleného přístupu k síti
- e) Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů

Primárně je tato politika určena pro vedení Nemocnice Strakonice, a.s., pro manažera kybernetické bezpečnosti a oddělení informačních technologií.

6.2 PRAVIDLA A POSTUPY PRO ZAJIŠTĚNÍ BEZPEČNOSTI SÍŤE

1. Každá část komunikační sítě musí být dokumentovaná ve fyzické a logické vrstvě. Za vedení dokumentace odpovídá garant příslušného aktiva.
2. Správa sítě a síťových prvků je oddělena od správy pracovních stanic a serverů.
3. Síť je segmentována a logicky oddělena za účelem zajištění bezpečnosti prvků ICT systémů a odolnosti vůči případným útokům.

6.3 URČENÍ PRÁV A POVINNOSTÍ ZA BEZPEČNÝ PROVOZ SÍŤE

1. Garant podpůrného aktiva je odpovědný za efektivní využití všech dostupných bezpečnostních funkcí používaných technologií.
2. Garant podpůrného aktiva stanoví odpovědnosti za správu bezpečnosti sítě.
3. Garant podpůrného aktiva zajistí dodržení principu oddělení rolí správy sítí a správy IS.
4. Architekt KB posuzuje nastavení a změny bezpečnosti provozu sítě a navrhuje opatření k zajištění bezpečného provozu sítě.

6.4 PRAVIDLA A POSTUPY PRO ŘÍZENÍ PŘÍSTUPŮ V RÁMCI SÍŤE

1. Pravidla jsou aplikovatelná na všechny komunikační sítě ve správě Nemocnice Strakonice, a.s. alespoň v rozsahu:
 - a) interní síť LAN
 - b) externí síť WAN
 - c) propojení na externí síť (Internet).
2. Pravidla pro řízení přístupu se aplikují na všechny segmenty sítě LAN.
3. Pro přístupy uživatelů a administrátorů do vnitřní sítě jsou použity nástroje pro správu a ověření identity.
4. Pro přístupy technických prostředků do vnitřní sítě jsou použity nástroje pro správu přístupu technických prostředků.
5. Přístupy jsou řízeny v jednotlivých prvcích ICT na základě skupin a rolí.

6.5 PRAVIDLA A POSTUPY PRO OCHRANU VZDÁLENÉHO PŘÍSTUPU K SÍTI

1. Vzdálený přístup uživatelů k sítím je řízen prostřednictvím odpovídajících technických prostředků.
2. Přístup z externích sítí je možný jen do demilitarizovaných zón (DMZ) navržených tak, aby případný vnější útok neohrozil bezpečnost interní sítě.
3. Vzdálený přístup je možný jen prostřednictvím komunikačního kanálu chráněného kryptografickými prostředky.
4. Vzdálené připojení dodavatelů je možné jen na základě oboustranné dohody, jejímž obsahem je povinně vzájemně akceptovaná bezpečnostní politika a výsledky analýzy rizik vyplývající z tohoto připojení.
5. Ověření identity žadatele o vzdálený přístup je provedeno formou vícefaktorové autentizace.

6.6 PRAVIDLA A POSTUPY PRO MONITOROVÁNÍ SÍTĚ A VYHODNOCOVÁNÍ PROVOZNÍCH ZÁZNAMŮ

1. Prvky ICT jsou trvale monitorovány.
2. Záznamy událostí prvků ICT je nutné uchovávat nejméně po dobu vyžadovanou zvláštním právním předpisem¹, nejméně však po dobu 12 měsíců.
3. Záznamy událostí musí být zajištěny před neoprávněným přístupem a neoprávněnou modifikací.
4. Všechny prvky ICT jsou napojeny na určený zdroj přesného času a jsou nejméně jednou za den synchronizovány.

7 PRAVIDLA CHOVÁNÍ DODAVATELŮ V OBLASTI BEZPEČNOSTI INFORMACÍ

Nemocnice Strakonice, a.s. (dále jen „Nemocnice“) požaduje, aby všichni její dodavatelé dodržovali stanovená pravidla v souladu s platnou politikou bezpečnosti informací. Nemocnice vykonává činnost jako poskytovatel základní služby podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

7.1 ZÁKLADNÍ PRAVIDLA

Dodavatel je povinen dodat plnění bez jakýchkoli právních či faktických vad a v souladu se všemi relevantními technickými a bezpečnostními normami.

Přístup k informačním a komunikačním prostředkům (ICT) Nemocnice je umožněn výhradně prostřednictvím autentizačních údajů přidělených samotnou nemocnicí.

Dodavatel musí nemocnici včas informovat o jakýchkoli hrozbách, poruchách nebo rizicích spojených s plněním.

Získané informace musí být chráněny před ztrátou, neoprávněným přístupem a zneužitím.

Dodavatel je povinen plně respektovat příslušné právní předpisy, včetně GDPR.

Náklady na implementaci bezpečnostních opatření nese dodavatel.

7.2 ZABEZPEČENÍ KOMUNIKACE

Jakákoli ztráta nebo odcizení dat, zařízení či softwaru musí být ihned nahlášena IT oddělení nemocnice – a to současně e-mailem i telefonicky.

Při práci na zařízeních připojených do nemocniční sítě je nezbytné dodržovat předepsaná bezpečnostní pravidla. Práce na serverech podléhá přísnému dohledu – včetně aktualizací, vedení dokumentace a zákazu neautorizovaných zásahů. Zaměstnanci dodavatele nesmí zneužívat síťovou infrastrukturu, šířit škodlivý software, skrývat svou identitu ani monitorovat síť bez oprávnění.

¹ 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).

7.3 KYBERNETICKÉ UDÁLOSTI A INCIDENTY

Dodavatel je povinen poskytovat plnou součinnost při řešení bezpečnostních incidentů. Jakékoli podezření na bezpečnostní incident musí být okamžitě oznámeno Manažerovi kybernetické bezpečnosti – vždy telefonicky i e-mailem.

7.4 POŽADAVKY NA INFORMAČNÍ SYSTÉMY

Dodané systémy musí zajistit ochranu důvěrnosti, integrity a dostupnosti dat. Veškeré operace v systému musí být zaznamenány v logu s jednoznačnou identifikací uživatele. Je nutné vynucovat používání silných hesel (minimálně 12 znaků); po 10 chybných pokusech o přihlášení má být přístup zablokován. Každý uživatel musí disponovat vlastním účtem – sdílené přihlašovací údaje jsou zakázány. Systém nesmí obsahovat komponenty s nevyřešenými bezpečnostními zranitelnostmi s CVE skóre vyšším než 3. Musí být zajištěny auditní záznamy, řízení přístupových práv, kontrola vstupních dat a testování softwaru v odděleném prostředí.

7.5 DODÁVKY

Software musí být smluvně upraven, dodán včetně zdrojových kódů a opatřen jasně definovanými licencemi. Hardware musí být předáván na základě protokolu podepsaného oběma stranami. Služby podléhají monitoringu a musí být dokumentována jejich kvalita a rozsah. Dokumentace musí být aktuální, vyhotovená v češtině (nebo angličtině u technických dokumentů), a tvoří nedílnou součást každé dodávky. Její absence může být důvodem k reklamaci nebo ukončení smlouvy.

7.6 FYZICKÁ BEZPEČNOST

Vstup nepovolaných osob do neveřejných prostor nemocnice je bez doprovodu zaměstnance zakázán. Přístup do datových center je možný pouze se souhlasem nemocnice; v blízkosti ICT vybavení je zakázáno jíst, pít nebo kouřit. Bez předchozí autorizace není povoleno odvážet či měnit zařízení.

7.7 ZAPOJENÍ PODDODAVATELŮ

Všichni poddodavatelé musí respektovat stejné bezpečnostní podmínky jako hlavní dodavatel. Nové poddodavatele lze zapojit pouze s písemným souhlasem nemocnice. Na výzvu je nutné doložit smlouvy s poddodavateli, potvrzující jejich závazek dodržovat požadovaná pravidla.

7.8 POSKYTOVÁNÍ INFORMACÍ TŘETÍM STRANÁM

Dodavatel je vázán povinností mlčenlivosti i po ukončení smluvního vztahu. Jakékoli zveřejnění informací o předmětu plnění či spolupráci s nemocnicí je možné výhradně s předchozím písemným souhlasem.

7.9 PORUŠENÍ PRAVIDEL

Nedodržení těchto pravidel představuje porušení smlouvy. V případě závažného nebo opakovaného porušení má nemocnice právo od smlouvy odstoupit a požadovat náhradu vzniklé škody.

Komunikační kanály

Technická zranitelnost: hlásit na e-mail: informatika@nemst.cz a telefon: +420 383 314 219.

Řízení rizik a bezpečnostní incidenty: kontaktovat Manažera kybernetické bezpečnosti na blazejovsky@jckb.cz.

MUDr. Bc. Tomáš Fiala, MBA