Nemocnice Pardubického kraje, a.s.
Kyjevská 44, 532 03 Pardubice
IČ: 275 20 536

POLITIKA BEZPEČNOSTI INFORMACÍ NEMOCNICE PARDUBICKÉHO KRAJE, a.s.

Poskytování zdravotních služeb je významnou měrou závislé na shromažďování a zpracování informací vztahujících se na údaje o pacientech, o zaměstnancích a o ostatních spolupracujících subjektech.
Systém managementu bezpečnosti informací ISMS (Information Security Management Systems) umožňuje realizaci systému řízení orientovaného na ochranu tzv. informačních aktiv. Pro dosažení tohoto cíle se řídíme metodikou podle mezinárodní normy ČSN ISO/IEC 27001. Odpovědnost za bezpečnost informací v organizaci má každý jednotlivý zaměstnanec.
ISMS je uplatňován proto, aby byla společnost schopna vyhodnocovat rizika a uplatňovat náležité kontrolní a řídící mechanismy k zachování důvěrnosti, integrity a dostupnosti informací.

Základním cílem je chránit informační aktiva společnosti.

11. principů politiky bezpečnosti informací

1. **Princip soukromí.** Soukromí dat je závislé především na zachování důvěrnosti osobních zdravotních údajů pacientů, osobních dat našich zaměstnanců a jiných partnerů. V rámci integrity dat je pro nás nejdůležitějším principem mlčenlivost a bezpečná pravidla pro osobní, písemnou a elektronickou komunikaci.
2. **Princip dostupnosti**. Dostupnost a sdílení dat je z pohledu péče o pacienty velmi důležité. Nastavujeme bezpečnou a vysokou úroveň dostupnosti dat.
3. **Princip bezpečnosti.** Jako každý systém je i zdravotní informační systém vystavován riziku síťových útoků zvenčí, ale také z řad uživatelů uvnitř společnosti. Je důležité věnovat zvýšenou pozornost nastavení zabezpečení a eliminovat možné ataky v systému. Chráníme informace během jejich vstupu, zpracování, uložení, přenosu a výstupu proti ztrátě důvěrnosti. Požadavky na bezpečnost informací řešíme s každým dodavatelem, který může přistupovat k informacím společnosti nebo zajišťuje prvky ICT infrastruktury.
4. **Princip ochrany.** Chráníme klíčové procesy před poškozením a informace před zcizením a následným zneužitím. Prosazujeme systém řízeného přístupu k informacím, fyzického přístupu do prostorů a bezpečnostní pravidla pro přenosná počítačová zařízení a jiné nosiče informací. Zajišťujeme ochranu aktiv, ke kterým mají přístup naši dodavatelé.
5. **Princip prevence.** Systematicky se zabýváme posuzováním možných rizik a oblast bezpečnosti informací kontrolujeme. Pro vytvoření strategie používáme podklady z analýzy informačního systému a auditů. Prevence bezpečnostních incidentů je pro nás zásadní. Prioritně řešíme vysoká rizika v souvislostech možných dopadů do celého systému bezpečnosti informací. Monitorujeme, hodnotíme a přezkoumáváme služby dodavatelů.
6. **Princip vědomí.** Uživatelé si musí být vědomi bezpečnostních hrozeb a otázek s nimi spjatých a být připraveni se podílet na dodržování politiky bezpečnosti informací a vzdělávat se v této oblasti. Kvalifikace zaměstnanců pověřených výkonem bezpečnostních rolí je systematicky rozvíjena. Politika bezpečnosti informací a související dokumentace je závazná pro všechny zaměstnance s přístupem k informacím, a to bez ohledu na zastávanou funkci, pozici či roli ve společnosti. Požadavky bezpečnosti informací komunikujeme s našimi dodavateli a dokumentujeme je v našich dohodách. Porušování zásad politiky bezpečnosti informací je bezpečnostní incident, který má vliv na bezpečnost informací se všemi důsledky z toho plynoucími.

7. **Princip praxe.** Zavádíme požadavky bezpečnostní politiky a standardů do praxe. Budování bezpečnosti je nikdy nekončící proces.
8. **Princip zdrojů.** Vytváříme podmínky k zajišťování všech zdrojů potřebných pro zavedení, udržování a rozvoj systému bezpečnosti informací. Plánované náklady na zajištění bezpečnosti informací jsou přidělovány a koordinovány vyváženě, odpovídají ceně informace vůči nákladům na jejich zabezpečení při dosažení efektivnosti vynaložených zdrojů.
9. **Princip rozvoje.** V souladu s moderními technologiemi a možnostmi zajišťujeme, udržujeme, chráníme a rozvíjíme informační majetky, spolehlivě zálohujeme informační systémy a zajišťujeme odpovídající ochranu shromažďovaných údajů v souladu s platnou legislativou. Naše procesy a činnosti spjaté s ochranou informací neustále zlepšujeme.
10. **Princip kontinuity.** Samotná bezpečnostní politika není neměnným dokumentem. Reagujeme na měnící se vnitřní a vnější prostředí a požadavky legislativy.
11. **Princip ochrany soukromí pacientů, návštěv a zaměstnanců.** Pravidla pořizování jakýchkoliv záznamů, viz. níže, se řídí příslušnými ustanoveními obecně závazných právních předpisů,
    - V areálech NPK je zakázáno pořizování video, foto či audiozáznamu (zákaz se vztahuje i na všechna oddělení a ambulance – vnitřní prostory) v případě, že by na záběrech měly figurovat jiné osoby než ty, které s tímto úkonem vyjádřily souhlas. Výjimku z uvedeného pravidla mají instituce disponující zpravodajskou licencí, pokud pořizují záznam pro zpravodajské účely.
    - Natáčení v porodnici je možné pouze se souhlasem vedoucího lékaře a výhradně tehdy, pokud je zaměřeno na matku, dítě a otce přítomného u porodu. Způsob jeho pořízení musí odpovídat tomu, že je prováděno za účelem zachycení a archivace události rodinného charakteru.
    - NPK může umožnit výjimku z uvedených pravidel v případě zdůvodněné žádosti, jež se adresuje na manažera bezpečnosti a krizového managementu.
    - Štáby či zástupci médií disponující zpravodajskou licencí musí o pořizování záznamů informovat tiskového mluvčího nemocnice, a to buď telefonicky (kontakt uveden na webových stránkách), nebo písemně na e-mail komunikace@nempk.cz.

MUDr. Tomáš Gottvald, MHA
generální ředitel a předseda představenstva Nemocnice Pardubického kraje, a.s.

V Pardubicích, 15. 10. 2024