Deklarace bezpečnostní politiky ÚHKT

I. Deklarace bezpečnostní politiky

Ústav hematologie a krevní transfuze (dále jen „**ÚHKT**“) jako největší hematologické centrum v Česku zajišťující prvotřídní medicínu a špičkový výzkum klade velký důraz na ochranu informací a služeb, což zajišťuje prostřednictvím Bezpečnostní politiky.

II. Odpovědnost

Odpovědnost za kybernetickou bezpečnost a Systém řízení bezpečnosti informací (dále i „**ISMS**“) nese na ÚHKT nejen vrcholové vedení, ale každý jednotlivý zaměstnanec, dodavatel a spolupracující subjekt.

III. Vize a cíle

1. Vizí je snížení a řízení kybernetických rizik ÚHKT tak, aby bylo zajištěno bezproblémové poskytování zdravotní péče pacientům a byly zajištěny podmínky pro bezpečný výzkum. Současně vybudování funkčního, pevného a vyváženého Systému řízení bezpečnosti informací, který respektuje základní účel fungování ÚHKT.
2. Cílem ÚHKT je zajistit dostatečnou ochranu důvěrnosti, integrity a dostupnosti všech zpracovávaných informací a poskytovaných služeb pro pacienty, zaměstnance a spolupracující subjekty za využití přiměřených a odpovídajících technických a organizačních opatření tak, aby byla zajištěna adekvátní úroveň kybernetické bezpečnosti.
3. Cíl je naplňován provozováním, kontrolováním, údržbou a neustálým zlepšováním Systému řízení bezpečnosti informací v kontextu rizik a požadavků dopadajících na ÚHKT v oblasti kybernetické bezpečnosti.

IV. Zaměstnanci

1. ÚHKT od svých zaměstnanců vyžaduje:
   a. důsledné dodržování stanovených pravidel, procesů a bezpečnostních opatření,
   b. aktivní spolupráci při udržování a zlepšování ISMS,
   c. hlášení bezpečnostních incidentů a událostí,
   d. pravidelné školení a zvyšování kompetencí a povědomí v oblasti kybernetické bezpečnosti,
   e. zajišťování ochrany aktiv.

V. Dodavatelé a spolupracující subjekty

1. ÚHKT od svých dodavatelů a spolupracujících subjektů vyžaduje:
   a. důsledné dodržování stanovených pravidel, procesů a bezpečnostních opatření,
   b. informování o bezpečnostních hrozbách, zranitelnostech, rizicích, událostech a incidentech, které mohou mít dopad na ÚHKT,
   c. aktivní a efektivní spolupráci při řešení bezpečnostních událostí a incidentů,
   d. zajišťování ochrany aktiv.

VI. Zásady a principy

1. Strategický a celistvý přístup

   a. Zajištění rovnovážného přístupu mezi základními atributy kybernetické bezpečnosti, kterými jsou lidé, procesy a technologie.
   b. Zajištění centrálního řízení Systému řízení bezpečnosti informací, který zahrnuje řízení kybernetické bezpečnosti, komunikaci a spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost, Ministerstvem zdravotnictví a řadou dalších institucí a spolupracujících subjektů.
   c. Podpora a propagace oblasti kybernetické bezpečnosti ze strany vrcholného vedení.

2. **Zajištění legislativního souladu**
   a. Dodržování a naplňování legislativních požadavků a vnitřních předpisů v oblasti kybernetické bezpečnosti.
3. **Přístup založený na riziku**
   a. Plánování a realizace bezpečnostních opatření za účelem minimalizace hrozeb, odstranění zranitelností a snižování úrovně rizik s ohledem na efektivitu, hospodárnost a soulad se stanovenou mírou přijatelnosti rizik.
   b. Zajišťování ochrany před kybernetickými útoky prostřednictvím průběžného sledování a vyhodnocování aktuálního vývoje a trendů hrozeb a jejich možných dopadů na ÚHKT.
4. **Akceptace prostředí**
   a. Postupné zavádění bezpečnostních opatření, pravidel a procesů kybernetické bezpečnosti tak, aby se plynule integrovaly a rozšířily v současné době zaběhlý provoz ÚHKT.
5. **Role a odpovědnosti**
   a. Definování a stanovení jasných rolí a odpovědnosti za účelem řízení kybernetické bezpečnosti.
   b. Podpora kolektivní a individuální odpovědnosti ve vytváření a udržování vyspělé kultury kybernetické bezpečnosti.
6. **Bezpečnostní opatření**
   a. Zajištění technických a organizačních opatření k ochraně před kybernetickými útoky, včasné reakci a rychlému zotavení.
   b. Zavádění vhodných bezpečnostních opatření, které budou zajišťovat dostatečnou úroveň kybernetické bezpečnosti a zároveň nebudou výrazně omezovat běžný provoz ÚHKT.
7. **Zvyšování bezpečnostního povědomí a komunikace**
   a. Školení v oblasti kybernetické bezpečnosti a zvyšování bezpečnostního povědomí o bezpečnostních hrozbách, pravidlech a bezpečnostních opatření zaměstnanců.
   b. Aktivní komunikace a naslouchání potřebám a požadavkům zaměstnanců.
   c. Kooperace a spolupráce se subjekty v oblasti zdravotnictví.
8. **Řízení dodavatelů**
   a. Řízení rizik spojených s dodavateli v rámci celého životního cyklu, stanovení jasných a přesných práv a povinností, zajišťování definování a kontroly bezpečnostních požadavků.
9. **Zajišťování kontinuity poskytovaných služeb**
   a. Zajišťování odolnosti vůči kybernetickým útokům a zajišťování kontinuity poskytovaných služeb a informací pacientům, zaměstnancům a dalším externím subjektům.
10. **Kontrola a neustálé zlepšování**
    a. Pravidelné hodnocení efektivity a dostatečnosti ISMS, provádění auditů a přezkoumávání stavu ISMS.
    b. Důslední dodržování, využívání a neustálé zlepšování vnitřních předpisů, pravidel, procesů a technických a organizačních opatření.

prof. MUDr. Petr Cetkovský, PhD, MBA

Digitálně podepsal prof. MUDr. Petr Cetkovský, PhD, MBA
Datum: 2025.03.13 12:51:00 +01'00'