Politika zabezpečení informací FN HK

Jedná se o bezpečnostní politiku, která odpovídá požadavkům § 30 Vyhlášky o kybernetické bezpečnosti. Tato politika je z hlediska její aktuálnosti pravidelně přezkoumávána a řízena Výborem pro řízení kybernetické bezpečnosti FN HK.

Tato politika definuje základní strategii a zásady týkající se informační bezpečnosti, určuje základní bezpečnostní pravidla pro provoz, používání a údržbu informačních a komunikačních technologií (dále jen „ICT“) s cílem zajistit požadovanou dostupnost a ochranu dat a osobních údajů (dále jen „informací“) a minimalizaci škod vzniklých v důsledku možných bezpečnostních incidentů.

Hlavní zásady práce s informacemi a způsob jejich zabezpečení:

- zajistit odpovídající ochranu informací v souladu s platnou legislativou,
- dodržovat přijatá organizační a technická opatření k ochraně informací,
- vytvářet a prosazovat systém řízeného přístupu k informacím,
- zajistit bezpečnou komunikaci a bezpečný přenos informací,
- začleňovat zabezpečení informací do odpovědnosti za práci,
- zajišťovat systematické vzdělávání a zvyšování kvalifikace zaměstnanců v oblasti bezpečnosti informací (kyberbezpečnost, ochrana osobních údajů),
- provádět stálou identifikaci bezpečnostních incidentů a přijímat účinná opatření pro zlepšení bezpečnosti informací,
- zpracovávat soubory opatření pro zachování kontinuity pro případy závažného výpadku v oblasti informací, tato opatření pravidelně přezkušovat a ověřovat,
- zabezpečovat informační systémy, internet, elektronickou poštu a další způsoby výměny informací,
- zabezpečovat systém fyzického přístupu do prostor pro snížení ohrožení informačního majetku,
- prosazovat politiku bezpečného pracoviště: pravidlo čistého stolu a uzamčené obrazovky monitoru,
- prosazovat bezpečnostní pravidla pro přenosná (mobilní) počítačová zařízení a jiné nosiče informací,
- zajišťovat spolehlivou kontrolu celé interní sítě proti působení škodlivého kódu (softwaru),
- udržovat a chránit informační majetky, spolehlivě zálohovat informační systémy,
- pravidelně monitorovat a vyhodnocovat bezpečnostní rizika,
- stanovovat dostatečně smluvní požadavky na zabezpečení informací ve vztahu ke třetím stranám.

Odpovědnost zaměstnanců (uživatelů ICT):

Každý, komu byl umožněn přístup k informačním prostředkům pro potřeby výkonu své pracovní nebo jiné schválené činnosti, přebírá odpovědnost za bezpečné nakládání s těmito prostředky a za ochranu informací ve své působnosti.

Všichni uživatelé ICT nesou v souladu s platnou legislativou a předpisy svůj podíl odpovědnosti za dodržení, resp. porušení pravidel, které se jich týkají. Všichni uživatelé ICT jsou povinni předepsaným způsobem reagovat na závady, poruchy a bezpečnostní incidenty, které se vyskytnou a upozornit na ně v souladu s příslušnými zásadami a předpisy.

Následky porušení bezpečnostní politiky:

Porušení zásad této politiky zabezpečení informací ze strany zaměstnanců a dalších uživatelů ICT je chápáno jako bezpečnostní incident, který má vliv na bezpečnost informací a v těchto intencích musí být řešen.

Příčiny porušení pravidel se musí analyzovat. Následně se musí přijímat účinná opatření s cílem poučení se z těchto událostí a zamezení opakovaného vzniku.

Schválil Výbor pro řízení kyberbezpečnosti dne 19. 1 .2023

MUDr. Aleš Herman, Ph.D., ředitel Fakultní nemocnice Hradec Králové

MUDr. Aleš Herman Ph.D.
Digitálně podepsal MUDr. Aleš Herman Ph.D.
Datum: 2023.02.08 09:37:53 +01'00'