Politika zabezpečení informací 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 s cílem zajistit požadovanou dostupnost a ochranu 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,
- vytvářet a prosazovat systém řízeného přístupu k informacím,
- zajistit zabezpečenou komunikaci a bezpečný přenos informací,
- začleňovat zabezpečení informací do odpovědnosti za práci,
- zajišťovat systematické vzdělávání a zvyšování kvalifikace zaměstnanců v oblasti bezpečnosti informací,
- provádět stálou identifikaci bezpečnostních incidentů a přijímat účinná opatření pro zlepšování 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 přístupných,
- zabezpečovat systém fyzického přístupu do prostor pro snížení ohrožení informačního majetku,
- prosazovat politiku bezpečného pracoviště: čistý stůl a prázdnou obrazovku,
- prosazovat bezpečnostní pravidla pro přenosná (mobilní) počítačová zařízení a jiné nosiče informací,
- zajišťovat spolehlivou kontrolu celé interní sítě proti působení škodlivého softwaru,
- udržovat a chránit informační majetky, spolehlivě zálohovat informační systémy.
- pravidelně monitorovat a vyhodnocovat bezpečnostní rizika,
- stanovovat dostatečné smluvní požadavky na zabezpečení informací ve vztahu ke třetím stranám

Odpovědnost zaměstnanců:

- Každý zaměstnanec, kterému byl umožněn přístup k informačním prostředkům pro potřeby výkonu pracovní činnosti, přebírá odpovědnost za bezpečné nakládání s těmito prostředky a za ochranu informací ve své působnosti.
- Všichni zaměstnanci nesou v souladu s platnou legislativou a předpisy svůj díl zodpovědnosti za dodržení, resp. porušení pravidel, které se jich týkají. Všichni zaměstnanci jsou povinni předepsaným způsobem reagovat na závady, poruchy a bezpečnostní incidenty, které se vyskytnou a upozornit na ně v souladu s příslušnými zásadami a směrnicemi.

Následky porušení informační politiky

- porušování zásad této politiky bezpečnosti informací ze strany zaměstnanců i dodavatelů je chápáno jako bezpečnostní incident, který má vliv na bezpečnost informací a v těchto intencích musí být řešen,
- příčiny porušení pravidel se musí analyzovat a přijímat účinná opatření s cílem učení se z těchto událostí a zamezení opakovaného vzniku.

Schválil: prof. MUDr. Vladimír Palička,CSc., dr. h. c., ředitel FN HK

dne 26.1.2017