Politika integrovaného systému řízení kvality a bezpečnosti informací

Politika integrovaného systému řízení kvality (QMS) a bezpečnosti informací (ISMS) Ústavu zdravotnických informací a statistiky České republiky (dále jen ústav) je plně podporována vrcholovým vedením v čele s ředitelem ústavu.

Základní principy činnosti ústavu:

- Nezávislost,
- Nestrannost,
- Transparentnost,
- Důvěryhodnost,
- Hospodárnost.

Strategie v oblasti řízení kvality (QMS dle ISO 9001):

- Poskytovat služby, které budou vždy kompletně naplňovat požadované a očekávané potřeby zřizovatele, veřejné správy a smluvních partnerů, při současném dodržování veškerých platných legislativních předpisů a norem týkajících se činnosti ústavu, procesů a činností systému managementu kvality.
- Uplatňovat princip neustálého zlepšování efektivnosti všech procesů integrovaného systému řízení.
- Udržovat a prohlubovat systém řízení kvality a jeho integrování do všech procesů ústavu na všech úrovních řízení.
- Usilovat o neustálé zlepšování procesů řízení zapojením všech zaměstnanců.
- Stabilizovat zaměstnance, rozšiřovat jejich způsobilost rozmanitou praxí a školeními, zvyšovat jejich spokojenost formou zlepšování pracovního prostředí, technické úrovně vybavení pracovišť a pracovních nástrojů a otevřenou komunikací mezi všemi pracovníky a vedením ústavu.

Strategie v oblasti bezpečnosti informací (ISMS dle ISO 27001):

- Respektovat všechny právní předpisy, standardy, normy a doporučení související s činností ústavu a procesy řízení bezpečnosti a ochrany informací.
- Trvale vytvářet podmínky k zajišťování všech zdrojů potřebných k zavedení, udržování a soustavnému zlepšování systému řízení bezpečnosti informací.
- Uplatňovat politiku založenou na principech důvěrnosti, dostupnosti a integrity informací, na dodržování právních a normativních předpisů a na smluvních požadavcích zainteresovaných stran.
- Zajistit bezpečnost informačních aktiv ústavu pomocí přiměřených a odpovídajících opatření.
- Pravidelně hodnotit plnění cílů a cílových hodnot vycházejících z analýzy rizik a této politiky.

- Prezentovat profesionální přístup a postavení ústavu přesným uplatňováním zásad informační bezpečnosti vůči smluvním partnerům a třetím stranám.
- Úroveň bezpečnosti nastavovat přiměřeně bezpečnostním rizikům a významu zajišťovaných aktivit. Rizika se hodnotí z hlediska vlivu na dosahování cílů ústavu, na dodržení úrovně poskytovaných služeb a z hlediska možných finančních a jiných dopadů na ústav.
- Prioritně zvládat vysoká rizika v souvislostech možných dopadů, významu zabezpečovaných aktivit a možností ústavu uvolnit potřebné zdroje. Proces řízení rizik je základním nástrojem předcházení škod.
- Systém řízení podrobovat soustavnému monitorování, vyhodnocování stavu bezpečnosti a zavádění adekvátních nápravných opatření. Preferuje se prevence bezpečnostních incidentů.
- Vědomí informační bezpečnosti je soustavně upevňováno a zaměstnanci jsou pravidelně proškolováni. Kvalifikace zaměstnanců pověřených výkonem bezpečnostních rolí je systematicky rozvíjena.

Při realizaci cílů politiky integrovaného systému řízení kvality a bezpečnosti informací očekává vedení ústavu od každého zaměstnance:

- Důsledné a přesné dodržování postupů stanovených interními dokumenty integrovaného systému řízení.
- Vysokou odpovědnost za jakost vlastní práce spočívající v předcházení chybám.
- Důslednou kontrolu výsledků své práce před jejich předáním spolupracovníkům nebo smluvním partnerům.

V Praze dne 1. července 2015

.....
doc. RNDr. Ladislav Dušek, Ph.D.
ředitel ústavu