Příloha č. 1 k Dílčí smlouvě č. 1

Klíčové činnosti MKB dle přílohy č. 5 Vyhlášky o KB – rozsah jejich realizace v rámci poskytované služby MKB

Uvedené činnosti budou realizovány na základě oboustranně dohodnutého časového harmonogramu v rozsahu smluvně dohodnutého období.

Klíčové činnosti MKB	Rozsah realizace ze strany NAKIT	Poznámka
a) Odpovědnost za řízení systému řízení bezpečnosti informací	Spolupracuje s vedením Nemocnice při implementaci požadavků zákona o KB do prostředí Nemocnice.	*NAKIT se výkonem této role nestává odpovědným za implementaci a neprovádí implementaci celého SŘBI /ISMS v Nemocnici, která je podle zákona o KB povinnou osobou – správcem základní služby a provozovatelem ISZS.* *Nemocnice je povinna smluvně zajistit auditora kybernetické bezpečnosti.*
b) Pravidelný reporting pro vrcholové vedení povinné osoby.	Pravidelný reporting pro vedení Nemocnice.	*V rozsahu plynoucích z požadavků Dílčí smlouvy na poskytnutí služby MKB.*
c) Pravidelná komunikace s vrcholovým vedením povinné osoby.	Pravidelná komunikace s vedením Nemocnice	*V rozsahu plynoucích z požadavků Dílčí smlouvy na poskytnutí služby MKB.*
d) Předkládání: ***- Zpráv o hodnocení aktiv a rizik,*** ***- Plánu zvládání rizik a*** ***- Prohlášení o aplikovatelnosti výboru pro řízení kybernetické bezpečnosti.***	Poskytuje podporu při zpracování uvedených dokumentů, pracovníky Nemocnice. Posuzuje materiály předložené jemu ze strany Nemocnice. Posouzené materiály předkládá Výboru.	*NAKIT se výkonem této role nestává odpovědným za implementaci a neprovádí implementaci celého SŘBI /ISMS v Nemocnici, která je podle zákona o KB povinnou osobou – správcem ZS a provozovatelem ISZS.*

e) Poskytování pokynů pro zajištění bezpečnosti informací při vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů v oblasti ICT.	Poskytuje podporu dotčeným útvarům Nemocnice, při zohlednění požadavků zákona o KB a vyhlášky KB v rámci vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů majících dopad na informační a kybernetickou bezpečnost nemocnice, do doby schválení interních řídících aktů – dokumentace SŘBI/ISMS Nemocnice. Poskytuje podporu při návrhu obsahu dokumentů vytvářejících či ukončujících dodavatelský vztah, či dokument takovýto vztah vybírající, hodnotící a řídící.	*NAKIT se výkonem této role nestává odpovědným za implementaci SŘBI/ISMS v Nemocnici, která je podle zákona o KB povinnou osobou – správcem ZS a provozovatelem ISZS.*
f) Komunikace s Úřadem, GovCERT/CSIRT.	Komunikace s Úřadem, GovCERT dle aktuální potřeby. Hlášení KBI a spolupráce při jejich řešení. Hlášení kontaktních údajů a jejich změn. Komunikace v rámci vydaných varování a bezpečnostních opatření vydaných Úřadem.	*Dle aktuální potřeby.*
g) Podílení se na procesu řízení rizik.	Spolupracuje s Nemocnicí ve smyslu posuzování navrhovaných dokumentů identifikace aktiv, hodnocení dopadů a řízení rizik. Posuzuje a následně předkládá ke schválení Výboru analýzy rizik předložené a zpracované ze strany Nemocnice, hodnocení dopadů a plány zvládání rizik.	*NAKIT se výkonem této role nestává odpovědným za implementaci SŘBI/ISMS v Nemocnici, která je podle zákona o KB povinnou osobou – správcem základní služby a provozovatelem ISZS.*
h) Koordinace řízení incidentů.	Spolupracuje na koordinaci a řízení KBI, za podpory poskytnuté bezpečnostními rolemi, pracovníky odboru IT Nemocnice a odborníkem na forenzní analýzu. Spolupracuje při tom s orgány činnými v trestním řízení a Úřadem.	*Nemocnice musí zajistit prosazování kompetencí MKB například prostřednictvím VŘKB.* *Nemocnice si musí smluvně zajistit specialistu na forenzní analýzu pro případ nutnosti řešit KBI.*
i) Vyhodnocování vhodnosti a účinnosti bezpečnostních opatření.	Posuzuje navrhovanou bezpečnostní dokumentaci SŘBI/ISMS Nemocnice. Spolupracuje s architektem KB na aktualizaci stávajících bezpečnostních opatření do doby schválení interních řídících aktů – dokumentace SŘBI/ISMS Nemocnice. Následně spolupracuje s architektem KB na případných návrzích změn architektury ISZS Nemocnice a posuzování významných změn s dopadem na KB v rámci akvizice, vývoje a údržby ISZS Nemocnice.	*NAKIT se výkonem této role nestává odpovědným za implementaci, celého SŘBI/ISMS v Nemocnici na Homolce, která je podle zákon o KB povinnou osobou – správcem základní služby a provozovatelem ISZS. Nemocnice si musí smluvně zajistit architekta KB.*

Pojmy uvedené v příloze odpovídají pojmům definovaných v Dílčí smlouvě, případně v Rámcové smlouvě o spolupráci v oblasti kybernetické bezpečnosti a příslušných právních předpisů. Nad rámec těchto pojmů jsou v příloze použity následující zkratky:

ZoKB - Zákon č. 181/2014 Sb. o kybernetické bezpečnosti
VyKB - Vyhláška č. 82/2108 Sb. o kybernetické bezpečnosti
ISZS - Informační systém základní služby
ZS - Základní služba
SŘBI - Systém řízení bezpečnosti informací
ISMS - Information Security management system (anglické synonymum k SŘBI – normalizovaný řadou norem ISO 27000)
NUKIB - Národní úřad pro kybernetickou bezpečnost
GovCERT - Vládní CERT = Computer Emergency Response Team – Tým pro reakci na počítačové hrozby
CSIRT **-** Národní CERT = Computer Security Incident Response Team – přijímá hlášení KB incidentů a poskytuje podporu řešení
Úřad **-** Národní úřad pro kybernetickou bezpečnost (NUKIB)
VŘKB **-** výbor pro řízení kybernetické bezpečnosti