Příloha č. 3 k Dílčí smlouvě č. 1

Přehled povinností správce základní služby a provozovatele ISZS plynoucích ze ZoKB a VyKB a rozdělení činností při jejich realizaci poskytováním služby MKB.

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

Rozdělení a popis činností					
P.č.	**zákon vyhláška**	**Ustanovení**	**Povinnosti a odpovědnosti stanovené ZoKB a VoKB**	**Nemocnice**	**NAKIT**
				Poskytovatel základní služby Správce a provozovatel ISZS	**Poskytovatel**
				Popis způsobu, rozsahu naplnění povinností stanovených legislativou	**Popis způsobu, rozsahu naplnění povinností stanovených legislativou**
ZoKB			**Zákon č. 181/2014 Sb. o kybernetické bezpečnosti**		
			Bezpečnostní opatření		
1	*ZoKB*	§ 4 odst. 2	**Zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti** informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, **informačního systému základní služb**y a významného informačního systému **a vést o nich bezpečnostní dokumentaci.**	Vlastními pracovníky či externím implementátorem navrhne a zavede SŘBI Nemocnice jejíž součástí je i stanovení bezpečnostních opatření, standardizuje povinné záznamy bezpečnostní dokumentace, určí odpovědnosti za jejich provádění vedení a reporting.	Poskytuje podporu vrcholovému vedení Nemocnice při implementaci požadavků ZoKB ve spolupráci s VŘKB a NUKIB.
2	*ZoKB*	§ 4 odst. 4	Zohlednit požadavky vyplývající z bezpečnostních opatření pří výběru dodavatele pro informační a komunikační systém a tyto	Vlastními pracovníky či externím implementátorem navrhne a zavede SŘBI Nemocnice jejíž součástí je i stanovení bezpečnostních požadavků na	Poskytuje podporu vrcholovému vedení Nemocnice při aplikaci požadavků na proces výběru dodavatele, hodnocení dodavatele, implementuje v souladu s

			požadavky zahrnout do uzavírané smlouvy.	proces výběru dodavatele, hodnocení dodavatele, implementuje v souladu s metodikou NUKIB požadavky na smluvní vztahy.	metodikou NUKIB požadavky na smluvní vztahy v rámci spolupráce ve VŘKB.
3	*ZoKB*	§ 4 odst. 5	Zajistit si ve smlouvě s dodavatelem cloud computingu dodržování bezpečnostních pravidel pro poskytování služeb cloud computingu stanovených Úřadem.	Vlastními pracovníky či externím implementátorem navrhne a zavede SŘBI Nemocnice jejíž součástí je i stanovení bezpečnostních požadavků na smluvní vztahy v oblasti cloud computingu.	Poskytuje podporu vrcholovému vedení Nemocnice při aplikaci požadavků na proces aplikace bezpečnostních požadavků a jejich implementaci v rámci spolupráce ve VŘKB.
4	*ZoKB*	§ 7 odst. 3	**Detekovat KBU** ve významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, **informačním systému základní služby** nebo významném informačním systému.	Zavede proces detekce a vyhodnocování KBU a jeho zavedení. Přidělí odpovědnosti a stanoví postupy pro detekci a vyhodnocování KBU. Definuje a aplikuje postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro jejich analýzu. Komunikuje informace o KBU v rámci uživatelů ISZS Nemocnice.	Na základě obdržené informace od Nemocnice o detekované KBU a informace z jejich vyhodnocení, poskytuje prostřednictvím VŘKB podporu vrcholovému vedení Nemocnice, při řešení KBU a vytváření návrhů na bezpečnostní opatření.
5	*ZoKB*	§ 8 odst. 1	**Hlásit KBI** ve významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, **informačním systému základní služby** nebo významném informačním systému.	Definuje a aplikuje postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu KBI. Komunikuje informace o KBI v rámci uživatelů ISZS Nemocnice. Zajistí spolupráci nezávislého odborníka na forenzní analýzu KBI. Spolupracuje s orgány činnými v trestním řízení. Schvaluje dokument hlášení KBI Úřadu.	Spolupracuje při koordinaci identifikace, sběru, získání a analýze KBI ve spolupráci s pracovníky odboru IT Nemocnice a odborníkem na forenzní analýzu. Poskytuje informace a podklady orgánům činným v trestní řízení k řešenému KBI. Zpracuje dokument hlášení o KBI, předkládá jej ke schválení vedení Nemocnice. Předává informaci VŘKB a DPO Nemocnice.
6	*ZoKB*	§ 8 odst. 4	Hlásit KBI Úřadu.	Poskytuje podporu při komunikaci s úřadem.	Komunikuje KBI bezodkladně po její detekci s Úřadem.

	ZoKB		**Opatření**		
5	*ZoKB*	§ 11 odst. 3	Provádět reaktivní opatření.	Je povinen zajistit provedení úřadem nařízených reaktivních opatřeních v NNH.	Ve spolupráci s VŘKB kontroluje provádění reaktivních opatření Koordinuje jejich realizaci, přijímá a shromažďuje hlášení o plnění obsahu reaktivního opatření ve stanovených termínech. Prostřednictvím Cestou VŘKB řídí nápravu v případě zjištěných nedostatků při realizaci reaktivních opatření. Zpracuje hlášení o plnění reaktivního opatření Úřadu a předkládá jej ke schválení vedení Nemocnice.
6	*ZoKB*	§ 11 odst. 4	Provádět ochranné opatření.	Je povinen provádět ochranná opatření vydaná Úřadem.	V případě povinnosti stanovené Úřadem komunikuje s Úřadem o provedení ochranného opatření a jeho výsledku.
	ZoKB		**Varování**		
7	*ZoKB*	§ 12 odst. 3	Úřad je z důvodu ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn po konzultaci s orgánem nebo osobou uvedenými v § 3 písm. c), d), f), g) nebo h), které jsou dotčeny kybernetickým bezpečnostním incidentem, veřejnost o tomto incidentu informovat nebo dotčenému orgánu nebo osobě uložit, aby tak učinil sám.	Přijímá od Úřadu varování v oblasti kybernetické bezpečnosti. Zajistí vyhodnocení, návrh a přijetí bezpečnostních opatření. Komunikuje tyto varování určeným pracovníkům, bezpečnostním rolím Nemocnice.	Sleduje varování vydaná Úřadem. Spolupracuje s VŘKB při návrhu bezpečnostních opatření.

8	*ZoKB*	§13 odst. 4	Oznámit Úřadu reaktivní opatření a jeho výsledek.	Poskytuje podporu při komunikaci s úřadem.	Bez zbytečného odkladu oznámí Úřadu provedení reaktivního opatření a jeho výsledek v souladu s VyKB.
9	*ZoKB*	§ 16 odst. 2	Kontaktní údaje a jejich změny oznamují orgány a osoby uvedené v § 3 písm. c) až g) Úřadu.	Zajistí určení a jmenování pracovníků Nemocnice do zákonem stanovených bezpečnostních rolí a poskytnutí potřebných údajů MKB pro hlášení kontaktních údajů a jejich případné změny Úřadu.	Zpracuje dokument hlášení kontaktních údajů a jejich změny Úřadu a komunikuje ji s Úřadem.
	ZoKB		**Nápravná opatření**		
10	*ZoKB*	§24 odst.1	Zjistí-li Úřad při kontrole nedostatky, uloží kontrolovanému orgánu nebo osobě, aby je ve stanovené lhůtě odstranila, popřípadě určí, jakým způsobem.	Zajistí odstranění Úřadem zjištěných nedostatků a popřípadě určí, jakým způsobem bude provedeno ve stanovené lhůtě.	Spolupracuje s VŘKB na stanovení opatření pro odstranění zjištěných nedostatků. Ve spolupráci s VŘKB kontroluje odstranění zjištěných nedostatků ve stanoveném termínu. Přijímá a shromažďuje hlášení o plnění úkolů k odstranění zjištěných nedostatků stanovených VŘKB. Komunikuje s Úřadem při řešení výsledků kontroly.
11	*ZoKB*	§ 24 odst. 2	**Pokud je** informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, **informační systém základní služby** nebo významný informační systém **pro zjištěné nedostatky bezprostředně ohrožen kybernetickým bezpečnostním incidentem, který jej může významně poškodit nebo zničit, může kontrolní orgán zakázat**	Zajistí přijetí opatření zákazu vydaného Úřadem k používání ISZS Nemocnice anebo jeho části do doby, než bude zjištěný nedostatek odstraněn.	Spolupracuje s VŘKB na stanovení opatření pro odstranění zjištěných nedostatků, které bezprostředně ohrožují KBI, který může ISZS Nemocnice nebo jeho část významně poškodit nebo zničit. Ve spolupráci s VŘKB kontroluje odstranění zjištěných nedostatků ve stanoveném termínu. Přijímá a shromažďuje hlášení o plnění úkolů k odstranění zjištěných nedostatků.

			kontrolovanému orgánu nebo osobě používání tohoto systému anebo jeho části do doby, než bude zjištěný nedostatek odstraněn.		Komunikuje s Úřadem při řešení výsledků kontroly.
	VyKB		**Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti**		
	VyKB		**Systém řízení bezpečnostní informací**		
	VyKB		**ISMS a organizační bezpečnost**		
12	*VyKB*	§ 3 odst. a)	Stanovit rozsah ISMS a určit v něm organizační části a aktiva, kterých se ISMS týká.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem.	Poskytuje součinnost VŘKB Při posuzování a schvalování dokumentace SŘBI/ISMS Nemocnice.
12	*VyKB*	§ 3 odst. b)	Stanovit cíle ISMS.		
12	*VyKB*	§ 3 odst. c)	Zavést přiměřená bezpečnostní opatření pro ISMS pro stanovený rozsah systému.		
12	*VyKB*	§ 3 odst. d)	Řídit rizika podle § 5 VyKB.		
12	*VyKB*	§ 3 odst. e)	Vytvořit a schválit bezpečnostní politiku ISMS.		
12	*VyKB*	§ 3 odst. f)	Zajistit provedení auditu kybernetické bezpečnosti.		
12	*VyKB*	§ 3 odst. g)	Zajistit pravidelné hodnocení účinnosti ISMS.		
12	*VyKB*	§ 3 odst. h)	Identifikovat a řídit významné změny.		

12	*VyKB*	§ 3 odst. i)	Aktualizovat ISMS a příslušnou dokumentaci.		
12	*VyKB*	§ 3 odst. j)	Řídit provoz a zdroje ISMS.		
	VyKB		**Organizační bezpečnost**		
	VyKB	§ 6 odst. 1 a)	Zajistit stanovení bezpečnostní politiky a cílů ISMS.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem. Zajistí dostatečné zdroje na implementaci SŘBI/ISMS. Zajistí dostatečné zdroje na aplikaci navržených a schválených bezpečnostních opatření informační a kybernetické bezpečnosti. určí a jmenuje stanovené bezpečnostní role, zajistí jim účinné kompetence, podporu a zdroje pro prosazování a realizaci stanovených bezpečnostních opatření informační a kybernetické bezpečnosti.	Poskytuje součinnost VŘKB při posuzování a schvalování dokumentace SŘBI/ISMS Nemocnice a její prosazovaní v Nemocnici.
	VyKB	§ 6 odst. 1 b)	Zajistit integraci ISMS do procesů povinné osoby.		
	VyKB	§ 6 odst. 1 c)	Zajistit dostupnost zdrojů potřebných pro ISMS.		
	VyKB	§ 6 odst. 1 d)	Informovat zaměstnance o významu ISMS a o významu dosažení shody s jeho požadavky se všemi dotčenými stranami.		
	VyKB	§ 6 odst. 1 e)	Zajistit podporu k dosažení zamýšlených výstupů ISMS.		
	VyKB	§ 6 odst. 1 f)	Vést zaměstnance k rozvíjení efektivity ISMS.		
	VyKB	§ 6 odst. 1 g)	Prosazovat neustálé zlepšování ISMS.		
	VyKB	§ 6 odst. 1 h)	Podporovat osoby zastávající bezpečnostní role při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti.		
	VyKB	§ 6 odst. 1 i)	Zajistit stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role.		
	VyKB	§ 6 odst. 1 j)	Zajistit zachování mlčenlivosti administrátorů a osob zastávajících bezpečnostní role.		

	VyKB	§ 6 odst. 1 k)	Zajistit pro osoby, které zastávají bezpečnostní role, příslušné pravomoci a zdroje.		
	VyKB	§ 6 odst. 1 l)	Zajistit testování plánu kontinuity činností, obnovy a procesů spojených se zvládáním KBI.		
	VyKB	§ 6 odst. 2	Určit složení VKB a bezpečnostní role a jejich práva a povinnosti související s ISMS.		
	VyKB	§ 6 odst. 3	Určit osoby, které budou zastávat bezpečnostní role.		
	VyKB		**Oblast akvizice, vývoje a údržby**		
	VyKB		**Řízení dodavatelů**		
	VyKB	§ 8 odst. 1 a)	Stanovit pravidla pro dodavatele.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem. Stanový proces stanovení bezpečnostních požadavků před výběrem dodavatele, hodnocení bezpečnostních požadavků v rámci procesu hodnocení zakázek. Zavede proces aplikace bezpečnostních požadavků na smluvní vztahy včetně zajištění kontinuity činností ISZS Nemocnice. zajistí aplikace požadavků průběžného bezpečnostního hodnocení dodavatelů a dopadů hodnocení na kontinuitu činností ISZS Nemocnice. Zavede proces auditu kybernetické bezpečnosti dodavatele.	Poskytuje podporu dotčeným útvarům Nemocnice, při zohlednění požadavků ZoKB a VyKB 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. Navrhuje obsah dokumentů vytvářejících či ukončujících dodavatelský vztah, či dokument takovýto vztah vybírající, hodnotící a řídící.
	VyKB	§ 8 odst. 1 b)	Vést evidenci svých významných dodavatelů.		
	VyKB	§ 8 odst. 1 c)	Prokazatelně písemně informovat své významné dodavatele o jejich evidenci.		
	VyKB	§ 8 odst. 1 d)	Seznamovat své dodavatele se stanovenými pravidly a požadovat dodržení těchto pravidel.		
	VyKB	§ 8 odst. 1 e)	Řídit rizika spojené s dodavateli.		
	VyKB	§ 8 odst. 1 f)	Zajistit, aby smlouvy uzavírané s významnými dodavateli obsahovaly informace uvedené v příloze č. 7 VyKB.		
	VyKB	§ 8 odst. 1 g)	Přezkoumávat plnění smluv s významnými dodavateli z hlediska ISMS.		
	VyKB	§ 8 odst. 2 a)	V rámci výběrového řízení a před uzavřením smlouvy provést		

			hodnocení rizik souvisejících s předmětem smlouvy.	zavede proces aplikace požadavků na cloud computing do smluvních vztahů.	
	VyKB	§ 8 odst. 2 b)	V rámci uzavíraných smluv stanovit způsoby a realizace bezpečnostního opatření. Určit obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.		
	VyKB	§ 8 odst. 2 c)	Provádět pravidelné hodnocení rizik a pravidelnou kontrolu bezpečnostních opatření.		
	VyKB	§ 8 odst. 2 d)	Zajistit řešení rizik a zjištěných nedostatků.		
	VyKB		**Akvizice, vývoj a údržba**		
	VyKB	§ 13 odst. a)	Řídit rizika podle § 5 VyKB.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem. Zajistí aplikaci požadavků ZoKB a VyKB v procesech identifikace a hodnocení aktiv, analýze a zvládání rizik a to jak v oblasti řízení interních procesů vývoje a údržby, tak v oblasti řízení akvizice vývoje a údržby smluvními dodavateli. Zajistí implementaci principů bezpečného vývoje u interního i externího vývoje. Zajistí testování významných změn, před jejich zavedením do produkčního prostředí.	Poskytuje podporu dotčeným útvarům Nemocnice, při zohlednění požadavků ZoKB a VyKB v rámci v procesech identifikace a hodnocení aktiv, analýze a zvládání rizik a to jak v oblasti řízení interních procesů vývoje a údržby, tak v oblasti řízení akvizice vývoje a údržby smluvními dodavateli, bezpečným vývojem a testování před nasazením do produkčního prostředí.
	VyKB	§ 13 odst. b)	Řídit významné změny podle § 11.		
	VyKB	§ 13 odst. c)	Stanovit bezpečnostní požadavky.		
	VyKB	§ 13 odst. d)	Zahrnout stanovené požadavky do projektu akvizice, vývoje a údržby.		
	VyKB	§ 13 odst. e)	Zajistit bezpečnost vývojového a testovacího prostředí a ochranu používaných testovacích dat.		
	VyKB	§ 13 odst. f)	Provádět bezpečnostní testování významných změn před jejich uvedením do provozu.		
	VyKB	§ 13 odst. g)	Plnit požadavek podle § 19 odst. 3, je-li cílem provedení akvizice nebo vývoje nástroj pro správu a ověřování identity.		
	VyKB		**Řízení změn**		
	VyKB	§ 11 odst. 1 a)	Přezkoumávat možné dopady změn.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními	Spolupracuje s VŘKB na ověřování plnění požadavků na řízení změn. Dotčeným
	VyKB	§ 11 odst. 1 b)	Určovat významné změny.		

	VyKB	§ 11 odst. 2 a)	Dokumentovat řízení významných změn.	zaměstnanci nebo externím implementátorem. Zajistí aplikaci požadavků na řízení celého životního cyklu změny. Zajistí penetrační testování významných změn, před jejich zavedením do produkčního prostředí, nezávislým externím subjektem.	útvarům poskytuje podporu při realizaci požadavků na řízení změn.
	VyKB	§ 11 odst. 2 b)	Provádět analýzu rizik.		
	VyKB	§ 11 odst. 2 c)	Přijímat opatření za účelem snížení všech nepříznivých dopadů významných změn.		
	VyKB	§ 11 odst. 2 d)	Aktualizovat bezpečnostní politiku a dokumentaci.		
	VyKB	§ 11 odst. 2 e)	Zajistit testování významných změn.		
	VyKB	§ 11 odst. 2 f)	Zajistit možnost navrácení do původního stavu.		
	VyKB	§ 11 odst. 3	Rozhodovat o penetračním testování nebo testování zranitelností.		
	VyKB		**Řízení aktiv a rizik**		
	VyKB		**Řízení aktiv**		
	VyKB	§ 4 odst. 1 a)	Stanovit metodiku pro identifikaci aktiv.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem.	Spolupracuje s VŘKB na ověřování plnění požadavků na řízení aktiv. Dotčeným útvarům poskytuje podporu při realizaci požadavků na řízení aktiv.
	VyKB	§ 4 odst. 1 b)	Stanovit metodiku pro hodnocení aktiv.		
	VyKB	§ 4 odst. 1 c)	Identifikovat a evidovat aktiva.		
	VyKB	§ 4 odst. 1 d)	Určit a evidovat garanty aktiv.		
	VyKB	§ 4 odst. 1 e)	Hodnotit a evidovat primární aktiva z hlediska důvěrnosti, integrity a dostupnosti.		
	VyKB	§ 4 odst. 1 f)	Určit a evidovat vazby mezi primárními a podpůrnými aktivy.		
	VyKB	§ 4 odst. 1 g)	Hodnotit podpůrná aktiva.		
	VyKB	§ 4 odst. 1 h)	Stanovit a zavádět pravidla ochrany pro jednotlivé úrovně aktiv.		

	VyKB	§ 4 odst. 1 i)	Stanovit přípustné způsoby používání aktiv a pravidla pro manipulaci s aktivy.		
	VyKB	§ 4 odst. 1 j)	Určit způsob likvidace dat, provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat.		
	VyKB	§ 4 odst. 2 a)	Posoudit rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství.		
	VyKB	§ 4 odst. 2 b)	Posoudit rozsah dotčených právních povinností a jiných závazků.		
	VyKB	§ 4 odst. 2 c)	Posoudit rozsah narušení vnitřních řídících a kontrolních činností.		
	VyKB	§ 4 odst. 2 d)	Posoudit poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty.		
	VyKB	§ 4 odst. 2 e)	Posoudit dopady na poskytování důležitých služeb.		
	VyKB	§ 4 odst. 2 f)	Posoudit rozsah narušení běžných činností.		
	VyKB	§ 4 odst. 2 g)	Posoudit dopady na zachování dobrého jména nebo ochranu dobré pověsti.		
	VyKB	§ 4 odst. 2 h)	Posoudit dopady na bezpečnost a zdraví osob.		
	VyKB	§ 4 odst. 2 i)	Posoudit dopady na mezinárodní vztahy.		
	VyKB	§ 4 odst. 2 j)	Posoudit dopady na uživatele informačního a komunikačního systému.		
	VyKB		**Řízení rizik**		

	VyKB	§ 5 odst. 1 a)	Stanovit metodiku pro hodnocení rizik.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem.	Spolupracuje s VŘKB na ověřování plnění požadavků na řízení rizik. Dotčeným útvarům poskytuje podporu při realizaci požadavků na řízení rizik.
	VyKB	§ 5 odst. 1 b)	S ohledem na aktiva identifikovat relevantní hrozby a zranitelnosti.		
	VyKB	§ 5 odst. 1 c)	Provádět hodnocení rizik.		
	VyKB	§ 5 odst. 1 d)	Při hodnocení rizik zohlednit relevantní hrozby a zranitelnosti a posoudit možné dopady na aktiva.		
	VyKB	§ 5 odst. 1 e)	Zpracovat zprávu o hodnocení rizik.		
	VyKB	§ 5 odst. 1 f)	Zpracovat na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti.		
	VyKB	§ 5 odst. 1 g)	Zpracovat a zavést plán zvládání rizik.		
	VyKB	§ 5 odst. 1 h)	Zohledňovat některé atributy při hodnocení rizik v plánu zvládání rizik.		
	VyKB	§ 5 odst. 1 i)	Zavádět bezpečnostní opatření v souladu s plánem zvládání rizik.		
	VyKB		**Řízení provozu a komunikací**		
	VyKB	§ 10 odst. 1 a)	Stanovit práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem. Zajistí zpracování a aplikaci bezpečnostních požadavků SŘBI/ISMS do provozní dokumentace ISZS Nemocnice (jako jsou příručka bezpečnostního správce ISZS Nemocnice, administrátorských a uživatelských příruček ISZS Nemocnice a další).	Spolupracuje s VŘKB na posuzování implementace bezpečnostních požadavků pro řízení provozu v dokumentaci SŘBI/ISMS a v provozní dokumentaci pro řízení ICT (jako jsou příručka bezpečnostního správce ISZS Nemocnice, administrátorských a uživatelských příruček ISZS Nemocnice a další).
	VyKB	§ 10 odst. 1 b)	Stanovit pravidla a postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů.		
	VyKB	§ 10 odst. 1 c)	Stanovit pravidla a postupy pro sledování KBU a opatření pro		

			ochranu přístupu k záznamům o těchto událostech.		
	VyKB	§ 10 odst. 1 d)	Stanovit pravidla a postupy pro ochranu před škodlivým kódem.		
	VyKB	§ 10 odst. 1 e)	Stanovit pravidla a postupy pro řízení technických zranitelností.		
	VyKB	§ 10 odst. 1 f)	Zajistit spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory.		
	VyKB	§ 10 odst. 1 g)	Stanovit postupy řízení a schvalování provozních změn.		
	VyKB	§ 10 odst. 1 h)	Stanovit pravidla a postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.		
	VyKB	§ 10 odst. 1 i)	Stanovit pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu.		
	VyKB	§ 10 odst. 1 j)	Stanovit pravidla a postupy pro instalaci technických aktiv.		
	VyKB	§ 10 odst. 1 k)	Stanovit provádění pravidelného zálohování a kontroly použitelnosti provedených záloh.		
	VyKB	§ 10 odst. 1 l)	Stanovit pravidla a postupy pro zajištění bezpečnosti síťových služeb.		
	VyKB		**Řízení přístupu**		
	VyKB	§ 12 odst. 1	Řídit přístup k informačnímu a komunikačnímu systému a přijímat opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení a která brání ve	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem. Zajistí zpracování a aplikaci	Spolupracuje s VŘKB na posuzování implementace bezpečnostních požadavků pro řízení přístupu v dokumentaci SŘBI/ISMS v provozní dokumentaci pro řízení ICT (jako jsou

			zneužití těchto údajů neoprávněnou osobou.	bezpečnostních požadavků SŘBI/ISMS do provozní dokumentace ISZS Nemocnice (jako jsou příručka bezpečnostního správce ISZS Nemocnice, administrátorských a uživatelských příruček ISZS Nemocnice a další).	příručka bezpečnostního správce ISZS Nemocnice, administrátorských a uživatelských příruček ISZS Nemocnice a další) a řídících aktech Nemocnice. Ve spolupráci s VŘKB kontroluje a vymáhá jejich dodržování.
	VyKB	§ 12 odst. 2 a)	Řídit přístup na základě skupin a rolí.		
	VyKB	§ 12 odst. 2 b)	Přidělit všem uživatelům a administrátorům přístupová práva a oprávnění a jedinečný identifikátor.		
	VyKB	§ 12 odst. 2 c)	Řídit identifikátory, přístupová práva, oprávnění aplikací a technických účtů.		
	VyKB	§ 12 odst. 2 d)	Zavádět bezpečnostní opatření pro řízení přístupu k prostředkům informačního a komunikačního systému.		
	VyKB	§ 12 odst. 2 e)	Zavádět bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení a jiných technických zařízení, popřípadě i bezpečnostní opatření spojená s využitím technických zařízení, která povinná osoba nemá ve správě.		
	VyKB	§ 12 odst. 2 f)	Omezit přidělování privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce.		
	VyKB	§ 12 odst. 2 g)	Omezit a kontrolovat používání programových prostředků, které mohou být schopné překonat systémové nebo aplikační kontroly.		
	VyKB	§ 12 odst. 2 h)	Přidělovat a odebírat přístupová oprávnění v souladu s politikou řízení přístupu.		

	VyKB	§ 12 odst. 2 i)	Provádět pravidelné přezkoumání nastavení veškerých přístupových oprávnění včetně rozdělení do přístupových skupin a rolí.		
	VyKB	§ 12 odst. 2 j)	Využívat nástroj pro správu a ověřování identity a nástroj pro řízení oprávnění.		
	VyKB	§ 12 odst. 2 k)	Prosazovat, aby uživatelé používali privátních autentizačních informací a dodržovali stanovené postupy.		
	VyKB	§ 12 odst. 2 l)	Zajistit odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.		
	VyKB	§ 12 odst. 2 m)	Zajistit odebrání nebo změnu přístupových oprávnění při ukončení nebo změně smluvního vztahu.		
	VyKB	§ 12 odst. 2 n)	Dokumentovat přidělování a odebírání přístupových oprávnění.		
	VyKB		**Fyzická bezpečnost**		
	VyKB	§ 17 odst. a)	Předcházet poškození, krádeži nebo zneužití aktiv nebo porušení poskytování služeb informačního a komunikačního systému.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem. Zajistí zpracování a aplikaci bezpečnostních požadavků SŘBI/ISMS do provozní dokumentace ISZS Nemocnice (jako jsou příručka bezpečnostního správce ISZS Nemocnice,	Spolupracuje s VŘKB na posuzování implementace bezpečnostních požadavků pro fyzickou bezpečnost v dokumentaci SŘBI/ISMS v provozní dokumentaci pro řízení ICT (jako jsou příručka bezpečnostního správce ISZS Nemocnice, administrátorských a uživatelských příruček ISZS Nemocnice a další) a řídících aktech Nemocnice.
	VyKB	§17 odst. b)	Stanovit fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány a zpracovávány informace a umístěna technická aktiva informačního a komunikačního systému.		

	VyKB	§ 17 odst. c)	Přijímat nezbytná opatření a uplatňovat prostředky fyzické bezpečnosti u fyzického bezpečnostního perimetru.	administrátorských a uživatelských příruček ISZS Nemocnice a další).	Ve spolupráci s VŘKB kontroluje a vymáhá jejich dodržování.
	VyKB		**Bezpečnost komunikační sítě**		
	VyKB	§ 18 odst. a)	Zajistit segmentaci komunikační sítě.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem. Zajistí zpracování a aplikaci bezpečnostních požadavků SŘBI/ISMS do provozní dokumentace ISZS Nemocnice (jako jsou příručka bezpečnostního správce ISZS Nemocnice, administrátorských a uživatelských příruček ISZS Nemocnice a další).	Spolupracuje s VŘKB na posuzování implementace bezpečnostních požadavků pro bezpečnost komunikační sítě v dokumentaci SŘBI/ISMS v provozní dokumentaci pro řízení ICT (jako jsou příručka bezpečnostního správce ISZS Nemocnice, administrátorských a uživatelských příruček ISZS Nemocnice a další). Ve spolupráci s architektem KB a VŘKB a ostatními bezpečnostními rolemi posuzuje a doporučuje zlepšení aktuálního stavu.
	VyKB	§ 18 odst. b)	Zajistit řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě.		
	VyKB	§ 18 odst. c)	Zajistit pomocí kryptografie důvěrnost a integritu dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do komunikační sítě pomocí bezdrátových technologií.		
	VyKB	§ 18 odst. d)	Aktivně blokovat nežádoucí komunikaci.		
	VyKB	§ 18 odst. e)	Pro zajištění segmentace sítě a pro řízení komunikace mezi jejími segmenty využívat nástroj, který zajistí ochranu integrity sítě.		
	VyKB		**Správa o ověřování identit**		
	VyKB	§ 19 odst. 1	Používat nástroj pro správu a ověření identit uživatelů, administrátorů a aplikací komunikačního a informačního systému.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem.	Spolupracuje s VŘKB na posuzování implementace bezpečnostních požadavků pro bezpečnost správy a ověřování identit v dokumentaci SŘBI/ISMS v provozní dokumentaci pro

	VyKB		Využívat autentizační mechanismus. (2FA)		řízení ICT (jako jsou příručka bezpečnostního správce ISZS Nemocnice, administrátorských a uživatelských příruček ISZS Nemocnice a další). Ve spolupráci s VŘKB a bezpečnostními rolemi kontroluje a doporučuje zlepšení aktuálního stavu.
	VyKB		**Ochrana před škodlivým kódem**		
	VyKB	§ 21 odst. 1 a)	S ohledem na důležitost aktiv zajišťovat použití nástroje pro nepřetržitou automatickou ochranu.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem.	Spolupracuje s VŘKB na posuzování implementace bezpečnostních požadavků pro oblast ochrany před škodlivým kódem v dokumentaci SŘBI/ISMS v provozní dokumentaci pro řízení ICT (jako jsou příručka bezpečnostního správce ISZS Nemocnice, administrátorských a uživatelských příruček ISZS Nemocnice a další). Ve spolupráci s VŘKB a bezpečnostními rolemi kontroluje a doporučuje zlepšení aktuálního stavu.
	VyKB	§ 21 odst. 1 b)	Monitorovat a řídit používání výměnných zařízení a datových nosičů.		
	VyKB	§ 21 odst. 1 c)	Řídit automatické spouštění obsahu výměnných zařízení a datových nosičů.		
	VyKB	§ 21 odst. 1 d)	Řídit oprávnění ke spuštění kódu.		
	VyKB	§ 21 odst. 1 e)	Provádět pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem.		
	VyKB		**Kryptografické prostředky**		
	VyKB	§ 26 odst. a)	Používat aktuálně odolné kryptografické algoritmy a kryptografické klíče.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem, s ohledem na vydaná doporučení a metodiky NUKIB.	Spolupracuje s VŘKB na posuzování implementace bezpečnostních požadavků pro bezpečnost v oblasti použití kryptografických prostředků v dokumentaci SŘBI/ISMS v provozní dokumentaci pro řízení ICT (jako jsou příručka bezpečnostního správce ISZS
	VyKB	§ 26 odst. b)	Používat systém správy klíčů a certifikátů.		
	VyKB	§ 26 odst. c)	Prosazovat bezpečné nakládání s kryptografickými prostředky.		

	VyKB	§ 26 odst. d)	Zohledňovat doporučení v oblasti kryptografických prostředků vydaných Úřadem.		Nemocnice, administrátorských a uživatelských příruček ISZS Nemocnice a další). Ve spolupráci s VŘKB a bezpečnostními rolemi kontroluje a doporučuje zlepšení aktuálního stavu.
	VyKB		**Bezpečnost lidských zdrojů**		
	VyKB	§ 9 odst. 1 a)	Stanovit plán rozvoje bezpečnostního povědomí.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem.	Spolupracuje s VŘKB na posuzování implementace bezpečnostních požadavků pro bezpečnost v bezpečnost lidských zdrojů v dokumentaci SŘBI/ISMS v provozní dokumentaci pro řízení ICT (jako jsou příručka bezpečnostního správce ISZS Nemocnice, administrátorských a uživatelských příruček ISZS Nemocnice a další). Ve spolupráci s VŘKB a bezpečnostními rolemi kontroluje a doporučuje zlepšení aktuálního stavu.
	VyKB	§ 9 odst. 1 b)	Určit osoby zodpovědné za realizaci jednotlivých činností.		
	VyKB	§ 9 odst. 1 c)	V souladu s plánem rozvoje bezpečnostního povědomí zajistit poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení.		
	VyKB	§ 9 odst. 1 d)	Zajistit pravidelná odborná školení pro osoby zastávající bezpečnostní role.		
	VyKB	§ 9 odst. 1 e)	Zajistit pravidelná školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní.		
	VyKB	§ 9 odst. 1 f)	Zajistit kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.		
	VyKB	§ 9 odst. 1 g)	Zajistit předání odpovědnostní v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role.		

	VyKB	§ 9 odst. 1 h)	Hodnotit účinnost plánu rozvoje bezpečnostního povědomí.		
	VyKB	§ 9 odst. 1 i)	Určit pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel.		
	VyKB	§ 9 odst. 2	Vést evidence školení a osob, které je absolvovaly.		
	VyKB		**Řízení kontinuity činností**		
	VyKB	§ 23 odst. 1 a)	Ověřit a kontrolovat přenášená data v rámci komunikační sítě a mezi komunikačními sítěmi.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem. Zavede proces detekce a vyhodnocování KBU a jeho zavedení. Přidělí odpovědnosti a stanoví postupy pro detekci a vyhodnocování KBU. Definuje a aplikuje postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro jejich analýzu. Komunikuje informace o KBU v rámci uživatelů ISZS Nemocnice.	Po obdržení informací od Nemocnice o detekované KBU a o jejich vyhodnocení, poskytuje podporu VŘKB při řešení KBU a tvorbě návrhů na bezpečnostní opatření. Spolupracuje při zavedení bezpečnostních opatření.
	VyKB	§ 23 odst. 1 b)	Ověřit a kontrolovat přenášená data na perimetru komunikační sítě.		
	VyKB	§ 23 odst. 1 c)	Blokovat nežádoucí komunikaci.		
	VyKB	§ 23 odst. 2	Zajistit detekci KBU s ohledem na důležitost aktiv v rámci jednotlivých míst.		
	VyKB		**Sběr a vyhodnocení kybernetických bezpečnostní událostí**		
	VyKB	§ 24 odst. a)	Sbírat a vyhodnocovat události zaznamenané dle §22 a §23 VyKB.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem. Definuje a aplikuje postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu KBI. Komunikuje informace o KBI v rámci	Spolupracuje při koordinaci identifikace, sběru, získání a analýze KBI ve spolupráci s pracovníky ICT Nemocnice a odborníkem na forenzní analýzu. Poskytuje informace a podklady orgánům činným v trestním řízení k řešenému KBI. Zpracuje dokument hlášení o KBI, předkládá jej ke schválení vedení
	VyKB	§ 24 odst. b)	Vyhledávat a seskupovat související záznamy.		
	VyKB	§ 24 odst. c)	Poskytovat informace pro určené bezpečnostní role o detekovaných KBU.		
	VyKB	§ 24 odst. d)	Vyhodnocovat KBU s cílem identifikace KBU.		

	VyKB	§ 24 odst. e)	Omezit případy nesprávného vyhodnocení událostí pravidelnou aktualizací pravidel.	uživatelů ISZS Nemocnice. Zajistí spolupráci nezávislého odborníka na forenzní analýzu KBI. Spolupracuje s orgány činnými v trestním řízení. Schvaluje dokument hlášení KBI Úřadu.	Nemocnice. Předává informaci VŘKB a DPO Nemocnice.
	VyKB	§ 24 odst. f)	Využívat informace získané nástrojem pro sběr a vyhodnocení KBU pro optimální nastavení bezpečnostních opatření informačního a komunikačního systému.		
	VyKB		**Řízení kontinuity činností**		
	VyKB	§ 15 odst. a)	Stanovit práva a povinnosti administrátorů a osob zastávajících bezpečnostní role.	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem. Zajistí zpracování dokumentace plánování a řízení kontinuity činností ISZS Nemocnice.	Spolupracuje s VŘKB na posuzování a schvalování návrhu dokumentů řízení kontinuity činností ISZS Nemocnice.
	VyKB	§ 15 odst. b)	Pomocí hodnocení rizik a analýzy dopadů vyhodnotit a dokumentovat možné dopady KBI a posoudit možná rizika související s ohrožením kontinuity činností.		
	VyKB	§ 15 odst. c)	Na základě výstupů hodnotit rizika a analýzy dopadů a stanovit cíle řízení kontinuity činností.		
	VyKB	§ 15 odst. d)	Stanovit politiku řízení kontinuity činností.		
	VyKB	§ 15 odst. e)	Vypracovat, aktualizovat a pravidelně testovat plány kontinuity činností a havarijní plány související s provozováním informačního a komunikačního systému.		
	VyKB	§ 15 odst. f)	Realizovat opatření pro zvýšení odolnosti informačního a komunikačního systému vůči KBI a omezením dostupnosti.		
	VyKB		**Zvládání kybernetických bezpečnostních událostí a incidentů**		

	VyKB	§ 14 odst. 1 a)	Zavést proces detekce a vyhodnocování KBU a zvládání KBI	Zajistí implementaci požadavků ZoKB vytvořením SŘBI/ISMS, vlastními zaměstnanci nebo externím implementátorem.	Spolupracuje s VŘKB na posuzování a schvalování návrhu dokumentu definujících procesy detekce KBU a zvládání KBI.
	VyKB	§ 14 odst. 1 b)	Přidělení odpovědnosti a stanovení postupů.	Stanový odpovědnosti konkrétním pracovním pozicím, bezpečnostním rolím, zajistí zpracování pracovních postupů pro praktickou realizaci detekce KBU a zvládání KBI.	Ve spolupráci s VŘKB spolupracuje na návrhu určení odpovědností a posuzování a schvalování návrhu dokumentu pracovních postupů pro detekci KBU a zvládání KBI.
	VyKB	§ 14 odst. 1 c)	Definovat a aplikovat postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu KBI.	Zajistí definici postupů pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu KBI a zajistí vyčíslení potřebných zdrojů pro jejich aplikaci.	Spolupracuje s VŘKB na vyhodnocování návrhů postupů pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu KBI.
	VyKB	§ 14 odst. 1 d)	Zajistit detekci KBU.	Zajistí aplikaci schválených postupů pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu KBI. Zajistí zdroje pro aplikaci schválených postupů pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu KBI.	Spolupracuje s VŘKB na kontrole realizace detekce KBU a vyhodnocování informací získaných detekcí, jejich dostatečnosti a efektivnosti. Poskytuje VŘKB zpětnou vazbu formou návrhů na zlepšení.
	VyKB	§ 14 odst. 1 f)	Zajistit, že uživatelé, administrátoři, osoby zastávající bezpečnostní role, další zaměstnanci a dodavatelé budou oznamovat neobvyklé chování informačního a komunikačního systému.	V rámci implementace SŘBI/ISMS zavede procesy pro oznamování neobvyklé chování informačního a komunikačního systém (ISZS).	Spolupracuje s VŘKB na vyhodnocování zaznamenaných oznámení v rámci řešení problematiky KBU/KBI.
	VyKB	§ 14 odst. 1 g)	Zajistit posuzování KBU.	Zajistí analýzu detekovaných KBU a celý životní cyklus řízení KBU.	Poskytuje podporu VŘKB.
	VyKB	§ 14 odst. 1 h)	Zajistit zvládání KBI.	Zajistí zpracování dokumentace řízení KBI a plánování a řízení kontinuity činností ISZS Nemocnice.	Spolupracuje s VŘKB na posuzování a schvalování návrhu dokumentů řízení a zvládání KBI a řízení kontinuity činností ISZS Nemocnice.

	VyKB	§ 14 odst. 1 i)	Přijímat opatření pro odvrácení a zmírnění dopadu KBI.	Přijímá opatření.	Spolupracuje s VŘKB a bezpečnostními rolemi při návrhu bezpečnostních opatření pro odvrácení a zmírnění dopadu KBI.
	VyKB	§ 14 odst. 1 j)	Hlásit KBI.	Odpovídá za hlášení KBI úřadu	Po detekci KBI neprodleně hlásí vedení Nemocnice. Po detekci KBI neprodleně hlásí Úřadu. Zpracovává dokument Hlášení KBU, předkládá ke schválení vedení Nemocnice a odesílá Úřadu.
	VyKB	§ 14 odst. 1 k)	Vést záznamy o KBI a jejich zvládání.	Vede záznamy.	Koordinuje zvládání KBI a zajištění informací pro forenzní analýzu KBI. Spolupracuje s orgány činnými v trestním řízení. Shromažďuje podklady o zvládání KBI.
	VyKB	§ 14 odst. 1 l)	Prošetřit a určit příčiny KBI.	Zajistí nezávislého odborníka na forenzní analýzu informací a podkladů o KBI a zpracování Zprávu o vyhodnocení a určení příčin KBI.	Spolupracuje s nezávislým odborníkem na forenzní analýzu KBI, předkládá Zprávu o vyhodnocení a určení příčin KBI VŘKB a spolupracuje na jejím projednání a procesu řešení nápravy.
	VyKB	§ 14 odst. 1 m)	Vyhodnotit účinnost řešení KBI.	Zajistí formou auditu KB se zaměřením na realizovaná bezpečnostní opatření na řešení následků a mitigaci rizik z KBI.	Spolupracuje s VŘKB při návrhu opatření v případě potřeby reagovat na negativní výsledky auditu kybernetické bezpečnosti.
	VyKB		**Audit kybernetické bezpečnosti**		
	VyKB	§ 16 odst. 1 a)	Provádět a dokumentovat dodržování bezpečnostní politiky.	Zajistí určení a jmenování auditora KB, vlastním zaměstnancem nebo externím dodavatelem.	Spolupracuje s VŘKB při návrhu opatření v případě potřeby reagovat na negativní výsledky či doporučení auditu kybernetické bezpečnosti.
	VyKB	§ 16 odst. 1 b)	Posuzovat soulad bezpečnostních opatření s nejlepší praxí, právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu a komunikačnímu systému.		

	VyKB	**příl.č.5**	**Dokumentace**		
	VyKB		**Obsah bezpečnostní politiky a bezpečnostní dokumentace**		
	VyKB		1. Bezpečnostní politika	Zajistí zpracování dokumentace SŘBI/ISMS Nemocnice a implementaci požadavků ZoKB, vlastními zaměstnanci nebo externím implementátorem.	Spolupracuje s VŘKB na posuzování a schvalování zpracovaných návrhů dokumentace SČBI/ISMS Nemocnice.
	VyKB		1.1. Politika systému řízení bezpečnosti informací		
	VyKB		1.2. Politika řízení aktiv		
	VyKB		1.3. Politika organizační bezpečnosti		
	VyKB		1.4. Politika řízení dodavatelů		
	VyKB		1.5. Politika bezpečnosti lidských zdrojů		
	VyKB		1.6 Politika řízení provozu a komunikací		
	VyKB		1.7. Politika řízení přístupu		
	VyKB		1.8. Politika bezpečného chování uživatelů		
	VyKB		1.9. Politika zálohování a obnovy a dlouhodobého ukládání		
	VyKB		1.10. Politika bezpečného předávání a výměny informací		
	VyKB		1.11. Politika řízení technických zranitelností		
	VyKB		1.12. Politika bezpečného používání mobilních zařízení		

	VyKB		1.13. Politika akvizice, vývoje a údržby		
	VyKB		1.14. Politika ochrany osobních údajů		
	VyKB		1.15. Politika fyzické bezpečnosti		
	VyKB		1.16. Politika bezpečnosti komunikační sítě		
	VyKB		1.17. Politika ochrany před škodlivým kódem		
	VyKB		1.18. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí		
	VyKB		1.19. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí		
	VyKB		1.20. Politika bezpečného používání kryptografické ochrany		
	VyKB		1.21. Politika řízení změn		
	VyKB		1.22. Politika zvládání kybernetických bezpečnostních incidentů		
	VyKB		1.23. Politika řízení kontinuity činností		
	VyKB		2.1. Zpráva z auditu kybernetické bezpečnosti		
	VyKB		2.2. Zpráva z přezkoumání systému řízení bezpečnosti informací		
	VyKB		2.3. Metodika pro identifikaci a hodnocení aktiv a pro hodnocení rizik		
	VyKB		2.4. Zpráva o hodnocení aktiv a rizik		

	VyKB		2.5. Prohlášení o aplikovatelnosti		
	VyKB		2.6. Plán zvládání rizik		
	VyKB		2.7. Plán rozvoje bezpečnostního povědomí		
	VyKB		2.8. Evidence změn		
	VyKB		2.9. Hlášené kontaktní údaje		
	VyKB		2.10. Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků		
	VyKB	**Příl. č. 7**	**Řízení dodavatelů – bezpečnostní opatření pro smluvní vztahy**		
			Bezpečnostní opatření pro smluvní vztahy	Zajistí zapracování bezpečnostních opatření pro smluvní vztahy do dokumentace SŘBI/ISMS Nemocnice a implementaci požadavků ZoKB, vlastními zaměstnanci nebo externím implementátorem v souladu s doporučeními a metodikou NUKIB.	Spolupracuje s VŘKB na posuzování a schvalování zpracovaných návrhů dokumentace SČBI/ISMS Nemocnice.

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. Jsou-li určité pojmy definovány rozdílně v této příloze a shora uvedených smlouvách, má přednost definice uvedená v této příloze.

ZoKB – zákon č. 181/2014 Sb. o kybernetické bezpečnosti
VyKB – Vyhláška č. 82/2108 Sb. o kybernetické bezpečnosti
MKB – manažer kybernetické bezpečnosti
ISZS – Informační systém základní služby
SŘBI – Systém řízení bezpečnosti informací
ISMS – Information Security Management System, anglické synonymum k SŘBI, upravený řadou norem ISO 27000

NUKIB – Národní úřad pro kybernetickou bezpečnost
Úřad – Národní úřad pro kybernetickou bezpečnost
GovCERT – Vládní CERT (Computer Emergency Response Team), tj. tým pro reakci na počítačové hrozby
CSIRT – Národní CERT (Computer Security Incident Response Team), který přijímá hlášení KB incidentů a poskytuje podporu řešení
VŘKB – Výbor pro řízení kybernetické bezpečnosti
KBU – kybernetická bezpečnostní událost
KBI – kybernetický bezpečnostní incident
DPO – Data Protection Officer, tj. pověřenec pro ochranu osobních údajů