Příloha č. 2 k Dílčí smlouvě č. 1

Rozdělení odpovědností plynoucích poskytovateli ZS a správci ISZS ze zákona o KB a vyhlášky o KB při poskytování služby MKB.

Osobou, které se ukládají povinnosti v oblasti kybernetické bezpečnosti, je na základě § 3 zákona o KB písmene f) poskytovatel ZS a provozovatel ISZS, kterým je na základě rozhodnutí NUKIB čj.1705/2021-NUKIB-E/350 Nemocnice na Homolce. NAKIT při poskytování služby MKB spolupracuje při plnění povinností Nemocnice, plynoucích ze zákona o KB poskytovateli ZS a provozovateli ISZS.

Odpovědnost plynoucí z ustanovení zákona KB a vyhlášky o KB	zákon o KB	vyhláška o KB	Nemocnice	*NAKIT*
	ustanovení	ustanovení	*Poskytovatel ZS Provozovatel ISZS*	*Dodavatel*
Zákon o KB				
Bezpečnostní opatření				
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 služby a významného informačního systému a vést o nich bezpečnostní dokumentaci.	§ 4 odst. 2		X	S
Zohlednit požadavky vyplývající z bezpečnostních opatření pří výběru dodavatele pro informační a komunikační systém a tyto požadavky zahrnout do uzavírané smlouvy.	§ 4 odst. 4		X	S
Zajistit si ve smlouvě s dodavatelem cloud computingu dodržování bezpečnostních pravidel pro poskytování služeb cloud computingu stanovených Úřadem.	§ 4 odst. 5		X	S
Detekovat KBU ve významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému.	§ 7 odst. 3		X	S
Hlásit KBI ve významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému.	§ 8 odst. 1		X	S
Hlásit KBI Úřadu.	§ 8 odst. 4		X	S
Opatření				
Provádět reaktivní opatření.	§ 11 odst. 3		X	S

Provádět ochranné opatření	§ 11 odst. 4		X	S
Varování				
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.	§ 12 odst. 3		X	S
Oznámit Úřadu reaktivní opatření a jeho výsledek.	§ 13 odst. 4		X	S
Kontaktní údaje a jejich změny oznamují orgány a osoby uvedené v § 3 písm. c) až g) Úřadu.	§ 16 odst. 2		X	S
Nápravná opatření				
Zjistí-li Úřad při kontrole nedostatky, uloží kontrolovanému orgánu nebo osobě, aby je ve stanovené lhůtě odstranila, popřípadě určí, jakým způsobem.	§ 24 odst. 1		X	S
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 kontrolovanému orgánu nebo osobě používání tohoto systému anebo jeho části do doby, než bude zjištěný nedostatek odstraněn.	§ 24 odst. 2		X	S

Vyhláška o KB				
Systém řízení bezpečnostní informací				
ISMS a organizační bezpečnost				
Stanovit rozsah ISMS a určit v něm organizační části a aktiva, kterých se ISMS týká.		§ 3 odst. a)	X	S
Stanovit cíle ISMS.		§ 3 odst. b)	X	S
Zavést přiměřená bezpečnostní opatření pro ISMS pro stanovený rozsah systému.		§ 3 odst. c)	X	S
Řídit rizika podle §5 vyhlášky o KB.		§ 3 odst. d)	X	S
Vytvořit a schválit bezpečnostní politiku ISMS.		§ 3 odst. e)	X	S
Zajistit provedení auditu kybernetické bezpečnosti.		§ 3 odst. f)	X	S
Zajistit pravidelné hodnocení účinnosti ISMS.		§ 3 odst. g)	X	S
Identifikovat a řídit významné změny.		§ 3 odst. h)	X	S

Aktualizovat ISMS a příslušnou dokumentaci.		§ 3 odst. i)	X	S
Řídit provoz a zdroje ISMS.		§ 3 odst. j)	X	S
Organizační bezpečnost				
Zajistit stanovení bezpečnostní politiky a cílů ISMS.		§ 6 odst. 1 a)	X	S
Zajistit integraci ISMS do procesů povinné osoby.		§ 6 odst. 1 b)	X	S
Zajistit dostupnost zdrojů potřebných pro ISMS.		§ 6 odst. 1 c)	X	S
Informovat zaměstnance o významu ISMS a o významu dosažení shody s jeho požadavky se všemi dotčenými stranami.		§ 6 odst. 1 d)	X	S
Zajistit podporu k dosažení zamýšlených výstupů ISMS.		§ 6 odst. 1 e)	X	S
Vést zaměstnance k rozvíjení efektivity ISMS.		§ 6 odst. 1 f)	X	S
Prosazovat neustálé zlepšování ISMS.		§ 6 odst. 1 g)	X	S
Podporovat osoby zastávající bezpečnostní role při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti.		§ 6 odst. 1 h)	X	S
Zajistit stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role.		§ 6 odst. 1 i)	X	S
Zajistit zachování mlčenlivosti administrátorů a osob zastávajících bezpečnostní role.		§ 6 odst. 1 j)	X	S
Zajistit pro osoby, které zastávají bezpečnostní role, příslušné pravomoci a zdroje.		§ 6 odst. 1 k)	X	S
Zajistit testování plánu kontinuity činností, obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.		§ 6 odst. 1 l)	X	S
Určit složení VŘKB a bezpečnostní role a jejich práva a povinnosti související s ISMS.		§ 6 odst. 2	X	S
Určit osoby, které budou zastávat bezpečnostní role.		§ 6 odst. 3	X	S
Oblast akvizice, vývoje a údržby				
Řízení dodavatelů				
Stanovit pravidla pro dodavatele.		§ 8 odst. 1 a)	X	S
Vést evidenci svých významných dodavatelů.		§ 8 odst. 1 b)	X	S
Prokazatelně písemně informovat své významné dodavatele o jejich evidenci.		§ 8 odst. 1 c)	X	S
Seznamovat své dodavatele se stanovenými pravidly a požadovat dodržení těchto pravidel.		§ 8 odst. 1 d)	X	S
Řídit rizika spojené s dodavateli.		§ 8 odst. 1 e)	X	S
Zajistit, aby smlouvy uzavírané s významnými dodavateli obsahovaly informace uvedené v příloze č. 7 vyhlášky o KB.		§ 8 odst. 1 f)	X	S
Přezkoumávat plnění smluv s významnými dodavateli z hlediska ISMS.		§ 8 odst. 1 g)	X	S

V rámci výběrového řízení a před uzavřením smlouvy provést hodnocení rizik souvisejících s předmětem smlouvy.		§ 8 odst. 2 a)	X	S
V rámci uzavíraných smluv stanovit způsoby a realizace bezpečnostního opatření. Určit obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.		§ 8 odst. 2 b)	X	S
Provádět pravidelné hodnocení rizik a pravidelnou kontrolu bezpečnostních opatření.		§ 8 odst. 2 c)	X	S
Zajistit řešení rizik a zjištěných nedostatků.		§ 8 odst. 2 d)	X	S
Akvizice, vývoj a údržba				
Řídit rizika podle § 5 vyhlášky o KB.		§ 13 odst. a)	X	S
Řídit významné změny podle § 11 vyhlášky o KB.		§ 13 odst. b)	X	S
Stanovit bezpečnostní požadavky.		§ 13 odst. c)	X	S
Zahrnout stanovené požadavky do projektu akvizice, vývoje a údržby.		§ 13 odst. d)	X	S
Zajistit bezpečnost vývojového a testovacího prostředí a ochranu používaných testovacích dat.		§ 13 odst. e)	X	S
Provádět bezpečnostní testování významných změn před jejich uvedením do provozu.		§ 13 odst. f)	X	S
Plnit požadavek podle § 19 odst. 3 vyhlášky o KB, je-li cílem provedení akvizice nebo vývoje nástroj pro správu a ověřování identity.		§ 13 odst. g)	X	S
Řízení změn				
Přezkoumávat možné dopady změn.		§ 11 odst. 1 a)	X	S
Určovat významné změny.		§ 11 odst. 1 b)	X	S
Dokumentovat řízení významných změn.		§ 11 odst. 2 a)	X	S
Provádět analýzu rizik.		§ 11 odst. 2 b)	X	S
Přijímat opatření za účelem snížení všech nepříznivých dopadů významných změn.		§ 11 odst. 2 c)	X	S
Aktualizovat bezpečnostní politiku a dokumentaci.		§ 11 odst. 2 d)	X	S
Zajistit testování významných změn.		§ 11 odst. 2 e)	X	S
Zajistit možnost navrácení do původního stavu.		§ 11 odst. 2 f)	X	S
Rozhodovat o penetračním testování nebo testování zranitelností.			X	S
Řízení aktiv a rizik				
Řízení aktiv				
Stanovit metodiku pro identifikaci aktiv.		§ 4 odst. 1 a)	X	S
Stanovit metodiku pro hodnocení aktiv.		§ 4 odst. 1 b)	X	S
Identifikovat a evidovat aktiva.		§ 4 odst. 1 c)	X	S

Určit a evidovat garanty aktiv.		§ 4 odst. 1 d)	X	S
Hodnotit a evidovat primární aktiva z hlediska důvěrnosti, integrity a dostupnosti.		§ 4 odst. 1 e)	X	S
Určit a evidovat vazby mezi primárními a podpůrnými aktivy.		§ 4 odst. 1 f)	X	S
Hodnotit podpůrná aktiva.		§ 4 odst. 1 g)	X	S
Stanovit a zavádět pravidla ochrany pro jednotlivé úrovně aktiv.		§ 4 odst. 1 h)	X	S
Stanovit přípustné způsoby používání aktiv a pravidla pro manipulaci s aktivy.		§ 4 odst. 1 i)	X	S
Určit způsob likvidace dat, provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat.		§ 4 odst. 1 j)	X	S
Posoudit rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství.		§ 4 odst. 2 a)	X	S
Posoudit rozsah dotčených právních povinností a jiných závazků.		§ 4 odst. 2 b)	X	S
Posoudit rozsah narušení vnitřních řídích a kontrolních činností.		§ 4 odst. 2 c)	X	S
Posoudit poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty.		§ 4 odst. 2 d)	X	S
Posoudit dopady na poskytování důležitých služeb.		§ 4 odst. 2 e)	X	S
Posoudit rozsah narušení běžných činností.		§ 4 odst. 2 f)	X	S
Posoudit dopady na zachování dobrého jména nebo ochranu dobré pověsti.		§ 4 odst. 2 g)	X	S
Posoudit dopady na bezpečnost a zdraví osob.		§ 4 odst. 2 h)	X	S
Posoudit dopady na mezinárodní vztahy.		§ 4 odst. 2 i)	X	S
Posoudit dopady na uživatele informačního a komunikačního systému.		§ 4 odst. 2 j)	X	S
Řízení rizik				
Stanovit metodiku pro hodnocení rizik.		§ 5 odst. 1 a)	X	S
S ohledem na aktiva identifikovat relevantní hrozby a zranitelnosti.		§ 5 odst. 1 b)	X	S
Provádět hodnocení rizik.		§ 5 odst. 1 c)	X	S
Při hodnocení rizik zohlednit relevantní hrozby a zranitelnosti a posoudit možné dopady na aktiva.		§ 5 odst. 1 d)	X	S
Zpracovat zprávu o hodnocení rizik.		§ 5 odst. 1 e)	X	S
Zpracovat na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti.		§ 5 odst. 1 f)	X	S
Zpracovat a zavést plán zvládání rizik.		§ 5 odst. 1 g)	X	S
Zohledňovat některé atributy při hodnocení rizik v plánu zvládání rizik.		§ 5 odst. 1 h)	X	S

Zavádět bezpečnostní opatření v souladu s plánem zvládání rizik.		§ 5 odst. 1 i)	X	S
Řízení provozu a komunikací				
Řízení provozu a komunikací				
Stanovit práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role.		§ 10 odst. 1 a)	X	S
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.		§ 10 odst. 1 b)	X	S
Stanovit pravidla a postupy pro sledování KBU a opatření pro ochranu přístupu k záznamům o těchto událostech.		§ 10 odst. 1 c)	X	S
Stanovit pravidla a postupy pro ochranu před škodlivým kódem.		§ 10 odst. 1 d)	X	S
Stanovit pravidla a postupy pro řízení technických zranitelností.		§ 10 odst. 1 e)	X	S
Zajistit spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory.		§ 10 odst. 1 f)	X	S
Stanovit postupy řízení a schvalování provozních změn.		§ 10 odst. 1 g)	X	S
Stanovit pravidla a postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.		§ 10 odst. 1 h)	X	S
Stanovit pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu.		§ 10 odst. 1 i)	X	S
Stanovit pravidla a postupy pro instalaci technických aktiv.		§ 10 odst. 1 j)	X	S
Stanovit provádění pravidelného zálohování a kontroly použitelnosti provedených záloh.		§ 10 odst. 1 k)	X	S
Stanovit pravidla a postupy pro zajištění bezpečnosti síťových služeb.		§ 10 odst. 1 l)	X	S
Řízení přístupu				
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 zneužití těchto údajů neoprávněnou osobou.		§ 12 odst. 1	X	S
Řídit přístup na základě skupin a rolí.		§ 12 odst. 2 a)	X	S
Přidělit všem uživatelům a administrátorům přístupová práva a oprávnění a jedinečný identifikátor.		§ 12 odst. 2 b)	X	S
Řídit identifikátory, přístupová práva, oprávnění aplikací a technických účtů.		§ 12 odst. 2 c)	X	S
Zavádět bezpečnostní opatření pro řízení přístupu k prostředkům informačního a komunikačního systému.		§ 12 odst. 2 d)	X	S
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.		§ 12 odst. 2 e)	X	S

Omezit přidělování privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce.		§ 12 odst. 2 f)	X	S
Omezit a kontrolovat používání programových prostředků, které mohou být schopné překonat systémové nebo aplikační kontroly.		§ 12 odst. 2 g)	X	S
Přidělovat a odebírat přístupová oprávnění v souladu s politikou řízení přístupu.		§ 12 odst. 2 h)	X	S
Provádět pravidelné přezkoumání nastavení veškerých přístupových oprávnění včetně rozdělení do přístupových skupin a rolí.		§ 12 odst. 2 i)	X	S
Využívat nástroj pro správu a ověřování identity a nástroj pro řízení oprávnění.		§ 12 odst. 2 j)	X	S
Prosazovat, aby uživatelé používali privátních autentizačních informací a dodržovali stanovené postupy.		§ 12 odst. 2 k)	X	S
Zajistit odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.		§ 12 odst. 2 l)	X	S
Zajistit odebrání nebo změnu přístupových oprávnění při ukončení nebo změně smluvního vztahu.		§ 12 odst. 2 m)	X	S
Dokumentovat přidělování a odebírání přístupových oprávnění.		§ 12 odst. 2 n)	X	S
Fyzická bezpečnost				
Předcházet poškození, krádeži nebo zneužití aktiv nebo porušení poskytování služeb informačního a komunikačního systému.		§ 17 odst. a)	X	S
Stanovit fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány a zpracovávány informace a umístěna technická aktiva informačního a komunikačního systému.		§ 17 odst. b)	X	S
Přijímat nezbytná opatření a uplatňovat prostředky fyzické bezpečnosti u fyzického bezpečnostního perimetru.		§ 17 odst. c)	X	S
Bezpečnost komunikační sítě				
Zajistit segmentaci komunikační sítě.		§ 18 odst. a)	X	S
Zajistit řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě.		§ 18 odst. b)	X	S
Zajistit pomocí kryptografie důvěrnost a integritu dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do komunikační sítě pomocí bezdrátových technologií.		§ 18 odst. c)	X	S
Aktivně blokovat nežádoucí komunikaci.		§ 18 odst. d)	X	S
Pro zajištění segmentace sítě a pro řízení komunikace mezi jejími segmenty využívat nástroj, který zajistí ochranu integrity sítě.		§ 18 odst. e)	X	S
Správa o ověřování identit				
Používat nástroj pro správu a ověření identit uživatelů, administrátorů a aplikací komunikačního a informačního systému.		§ 19 odst. 1	X	S

Využívat autentizační mechanismus.		§ 19 odst. 3	X	S
Ochrana před škodlivým kódem				
S ohledem na důležitost aktiv zajišťovat použití nástroje pro nepřetržitou automatickou ochranu.		§ 21 odst. 1 a)	X	S
Monitorovat a řídit používání výměnných zařízení a datových nosičů.		§ 21 odst. 1 b)	X	S
Řídit automatické spouštění obsahu výměnných zařízení a datových nosičů.		§ 21 odst. 1 c)	X	S
Řídit oprávnění ke spuštění kódu.		§ 21 odst. 1 d)	X	S
Provádět pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem.		§ 21 odst. 1 e)	X	S
Kryptografické prostředky				
Používat aktuálně odolné kryptografické algoritmy a kryptografické klíče.		§ 26 odst. a)	X	S
Používat systém správy klíčů a certifikátů.		§ 26 odst. b)	X	S
Prosazovat bezpečné nakládání s kryptografickými prostředky.		§ 26 odst. c)	X	S
Zohledňovat doporučení v oblasti kryptografických prostředků vydaných Úřadem.		§ 26 odst. d)	X	S
Bezpečnost lidských zdrojů				
Stanovit plán rozvoje bezpečnostního povědomí.		§ 9 odst. 1 a)	X	S
Určit osoby zodpovědné za realizaci jednotlivých činností.		§ 9 odst. 1 b)	X	S
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.		§ 9 odst. 1 c)	X	S
Zajistit pravidelná odborná školení pro osoby zastávající bezpečnostní role.		§ 9 odst. 1 d)	X	S
Zajistit pravidelná školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní.		§ 9 odst. 1 e)	X	S
Zajistit kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.		§ 9 odst. 1 f)	X	S
Zajistit předání odpovědnostní v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role.		§ 9 odst. 1 g)	X	S
Hodnotit účinnost plánu rozvoje bezpečnostního povědomí.		§ 9 odst. 1 h)	X	S
Určit pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel.		§ 9 odst. 1 i)	X	S
Vést evidence školení a osob, které je absolvovaly.		§ 9 odst. 2	X	S
Řízení kontinuity činností				

Detekce kybernetických bezpečnostních událostí				
Ověřit a kontrolovat přenášená data v rámci komunikační sítě a mezi komunikačními sítěmi.		§ 23 odst. 1 a)	X	S
Ověřit a kontrolovat přenášená data na perimetru komunikační sítě.		§ 23 odst. 1 b)	X	S
Blokovat nežádoucí komunikaci.		§ 23 odst. 1 c)	X	S
Zajistit detekci KBU s ohledem na důležitost aktiv v rámci jednotlivých míst.		§ 23 odst. 2	X	S
Sběr a vyhodnocení kybernetických bezpečnostní událostí				
Sbírat a vyhodnocovat události zaznamenané dle §22 a §23 VyKB.		§ 24 odst. a)	X	S
Vyhledávat a seskupovat související záznamy.		§ 24 odst. b)	X	S
Poskytovat informace pro určené bezpečnostní role o detekovaných KBU.		§ 24 odst. c)	X	S
Vyhodnocovat KBU s cílem identifikace KBU.		§ 24 odst. d)	X	S
Omezit případy nesprávného vyhodnocení událostí pravidelnou aktualizací pravidel.		§ 24 odst. e)	X	S
Využívat informace získané nástrojem pro sběr a vyhodnocení KBU pro optimální nastavení bezpečnostních opatření informačního a komunikačního systému.		§ 24 odst. f)	X	S
Řízení kontinuity činností				
Stanovit práva a povinnosti administrátorů a osob zastávajících bezpečnostní role.		§ 15 odst. a)	X	S
Pomocí hodnocení rizik a analýzy dopadů vyhodnotit a dokumentovat možné dopady kybernetických bezpečnostních incidentů a posoudit možná rizika související s ohrožením kontinuity činností.		§ 15 odst. b)	X	S
Na základě výstupů hodnotit rizika a analýzy dopadů a stanovit cíle řízení kontinuity činností.		§ 15 odst. c)	X	S
Stanovit politiku řízení kontinuity činností.		§ 15 odst. d)	X	S
Vypracovat, aktualizovat a pravidelně testovat plány kontinuity činností a havarijní plány související s provozováním informačního a komunikačního systému.		§ 15 odst. e)	X	S
Realizovat opatření pro zvýšení odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti.		§ 15 odst. f)	X	S
Zvládání kybernetických bezpečnostních událostí a incidentů				
Zavést proces detekce a vyhodnocování kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů		§ 14 odst. 1 a)	X	S
Přidělení odpovědnosti a stanovení postupů.		§ 14 odst. 1 b)	X	S
Definovat a aplikovat postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetických bezpečnostních incidentů.		§ 14 odst. 1 c)	X	S
Zajistit detekci kybernetických bezpečnostních událostí.		§ 14 odst. 1 d)	X	S

Zajistit, že uživatelé, administrátoři, osoby zastávající bezpečnostní role, další zaměstnanci a dodavatelé budou oznamovat neobvyklé chování informačního a komunikačního systému.		§ 14 odst. 1 f)	X	S
Zajistit posuzování kybernetických bezpečnostních událostí.		§ 14 odst. 1 g)	X	S
Zajistit zvládání kybernetických bezpečnostních incidentů.		§ 14 odst. 1 h)	X	S
Přijímat opatření pro odvrácení a zmírnění dopadu kybernetických bezpečnostních incidentů.		§ 14 odst. 1 i)	X	S
Hlásit KBI.		§ 14 odst. 1 j)	X	S
Vést záznamy o kybernetických bezpečnostních incidentech a jejich zvládání.		§ 14 odst. 1 k)	X	S
Prošetřit a určit příčiny kybernetických bezpečnostních incidentů.		§ 14 odst. 1 l)	X	S
Vyhodnotit účinnost řešení kybernetických bezpečnostních incidentů.		§ 14 odst. 1 m)	X	S
Audit kybernetické bezpečnosti				
Provádět a dokumentovat dodržování bezpečnostní politiky.		§ 16 odst. 1 a)	X	S
Posuzovat soulad bezpečnostních opatření s nejlepší praxí, právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu a komunikačnímu systému.		§ 16 odst. 1 b)	X	S
Dokumentace				
1. Bezpečnostní politika			X	S
1.1. Politika systému řízení bezpečnosti informací			X	S
1.2. Politika řízení aktiv			X	S
1.3. Politika organizační bezpečnosti			X	S
1.4. Politika řízení dodavatelů			X	S
1.5. Politika bezpečnosti lidských zdrojů			X	S
1.6 Politika řízení provozu a komunikací			X	S
1.7. Politika řízení přístupu			X	S
1.8. Politika bezpečného chování uživatelů			X	S
1.9. Politika zálohování a obnovy a dlouhodobého ukládání			X	S
1.10. Politika bezpečného předávání a výměny informací			X	S
1.11. Politika řízení technických zranitelností			X	S
1.12. Politika bezpečného používání mobilních zařízení			X	S
1.13. Politika akvizice, vývoje a údržby			X	S
1.14. Politika ochrany osobních údajů			X	S

1.15. Politika fyzické bezpečnosti			X	S
1.16. Politika bezpečnosti komunikační sítě			X	S
1.17. Politika ochrany před škodlivým kódem			X	S
1.18. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí			X	S
1.19. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí			X	S
1.20. Politika bezpečného používání kryptografické ochrany			X	S
1.21. Politika řízení změn			X	S
1.22. Politika zvládání kybernetických bezpečnostních incidentů			X	S
1.23. Politika řízení kontinuity činností			X	S
2.1. Zpráva z auditu kybernetické bezpečnosti			X	S
2.2. Zpráva z přezkoumání systému řízení bezpečnosti informací			X	S
2.3. Metodika pro identifikaci a hodnocení aktiv a pro hodnocení rizik			X	S
2.4. Zpráva o hodnocení aktiv a rizik			X	S
2.5. Prohlášení o aplikovatelnosti			X	S
2.6. Plán zvládání rizik			X	S
2.7. Plán rozvoje bezpečnostního povědomí			X	S
2.8. Evidence změn			X	S
2.9. Hlášené kontaktní údaje			X	S
2.10. Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků			X	S
Příloha č. 7 Řízení dodavatelů – bezpečnostní opatření pro smluvní vztahy			X	S

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:

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 NÚKIB
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
Výbor – Výbor pro řízení kybernetické bezpečnosti Nemocnice
X – označení pro určení odpovědnosti za plnění ustanovení příslušných právních předpisů
S – v rámci zajištění bezpečnostní role MKB spolupracuje s VŘKB a vrcholovým vedením Nemocnice při řízení kybernetické bezpečnosti a implementaci požadavků zákona o KB a vyhlášky o KB do dokumentace SŘBI/ISMS Nemocnice.