Název	Popis	ZoKB	VyKB	Odpovědost		Poznámka
		§, odstavec	§, odstavec	Objednatel	Poskytovatel	
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		
Stanovit cíle ISMS.			§ 3 odst. b)	X		
Zavést přiměřená bezpečnostní opatření pro ISMS pro stanovený rozsah systému.			§ 3 odst. c)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Řídit rizika podle § 5 VyKB.			§ 3 odst. d)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Vytvořit a schválit bezpečnostní politiku ISMS.	*Musí obsahovat zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti.*		§ 3 odst. e)	X		
Zajistit provedení auditu KB.			§ 3 odst. f)	X		
Zajistit pravidelné hodnocení účinnosti systému ISMS.	*Musí obsahovat hodnocení stavu ISMS včetně revize hodnocení rizik, posouzení výsledků provedených auditů KB a dopadů KBI na ISMS.*		§ 3 odst. g)	X		
Identifikovat a řídit významné změny.	*Podle § 11.*		§ 3 odst. h)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Aktualizovat ISMS a příslušnou dokumentaci.	*Na základě výsledků auditu KB, výsledků vyhodnocení účinnosti systému ISMS a v souvislosti s prováděnými významnými změnami.*		§ 3 odst. i)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Řídit provoz a zdroje ISMS.	*Zaznamenávat činnosti spojené s ISMS a řízením rizik.*		§ 3 odst. j)	X		
Organizační bezpečnost						
Zajistit stanovení bezpečnostní politiky a cílů ISMS.			§ 6 odst.1 a)	X		
Zajistit integraci ISMS do procesů povinné osoby.			§ 6 odst.1 b)	X		
Zajistit dostupnost zdrojů potřebných pro ISMS.			§ 6 odst.1 c)	X		
Informovat zaměstnance o významu ISMS a o významu dosažení shody s jeho požadavky se všemi dotčenými stranami.			§ 6 odst.1 d)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zajistit podporu k dosažení zamýšlených výstupů ISMS.			§ 6 odst.1 e)	X		
Vést zaměstnance k rozvíjení efektivity ISMS.			§ 6 odst.1 f)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Prosazovat neustálé zlepšování ISMS.			§ 6 odst.1 g)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Podporovat osoby zastávající bezpečnostní role při prosazování KB v oblastech jejich odpovědnosti.			§ 6 odst.1 h)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zajistit stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role.			§ 6 odst.1 i)	X		
Zajistit zachování mlčenlivosti administrátorů a osob zastávajících bezpečnostní role.			§ 6 odst.1 j)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zajistit pro osoby, které zastávají bezpečnostní role, příslušné pravomoci a zdroje.	*Včetně rozpočtových prostředků k naplňování jejich rolí.*		§ 6 odst.1 k)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zajistit testování plánu kontinuity činností, obnovy a procesů spojených se zvládáním KBI.			§ 6 odst.1 l)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Určit složení VKB a bezpečnostní role a jejich práva a povinnosti související s ISMS.			§ 6 odst.2	X		
Určit osoby, které budou zastávat bezpečnostní role.	*MKB, architekt KB, auditor KB, garant aktiva.*		§ 6 odst.3	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Oblast akvizice, vývoje a údržby						
Řízení dodavatelů						
Stanovit pravidla pro dodavatele.	*Zohledňovat požadavky ISMS.*		§ 8 odst.1 a)	X		
Vést evidenci svých významných dodavatelů.			§ 8 odst.1 b)	X		
Prokazatelně písemně informnovat své významné dodavatele o jejich evidenci.	*Náležitosti prokazatelného informování: identifikace správce/provozovatele, identifikace informačního a komunikačního systému, identifikace významného dodavatele, vyrozumění o skutečnosti, že dodavatel je pro správce významným dodavatelem (případně také o tom, že významný dodavatel je současně provozovatelem), obsah pravidel podle §8 odst.1 a).*		§ 8 odst.1 c)	X		
Seznamovat své dodavatele se stanovenými pravidly a požadovat dodržení těchto pravidel.	*Viz § 8 odst.1 a)*		§ 8 odst.1 d)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Řídit rizika spojené s dodavateli.			§ 8 odst.1 e)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zajistit, aby smlouvy uzavírané s významnými dodavateli obsahovaly informace uvedené v příloze č. 7 VyKB.	*Příloha č. 7 - Řízení dodavatelů - bezpečnostní opatření pro smluvní vztahy.*		§ 8 odst.1 f)	X		
Přezkoumávat plnění smluv s významnými dodavateli z hlediska ISMS.			§ 8 odst.1 g)	X		
V rámci výběrového řízení a před uzavřením smlouvy provést hodnocení rizik souvisejících s předmětem smlouvy.	*U významných dodavatelů.*		§ 8 odst.2 a)	X		
V rámci uzavíraných smluv stanovit způsoby a realizace bezpečnostního opatření. Určit obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.	*U významných dodavatelů.*		§ 8 odst.2 b)	X		
Provádět pravidelné hodnocení rizik a pravidelnou kontrolu bezpečnostních opatření.	*U významných dodavatelů.*		§ 8 odst.2 c)	X		

Zajistit řešení rizik a zjištěných nedostatků.	*U významných dodavatelů.*		§ 8 odst.2 d)	X		
Akvizice, vývoj a údržba						
Řídit rizika podle § 5 VyKB.	*V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému.*		§ 13 odst. a)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Řídit významné změny podle § 11.	*V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému.*		§ 13 odst. b)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Stanovit bezpečnostní požadavky.	*V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému.*		§ 13 odst. c)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zahrnout stanovené požadavky do projektu akvizice, vývoje a údržby.	*V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému.*		§ 13 odst. d)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zajistit bezpečnost vývojového a testovacího prostředí a ochranu používaných testovacích dat.	*V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému.*		§ 13 odst. e)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Provádět bezpečnostní testování významných změn před jejich uvedením do provozu.	*V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému.*		§ 13 odst. f)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Plnit požadavek podle § 19 odst.3, je-li cílem provedení akvizice nebo vývoje nástroj pro správu a ověřování identity.	*V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému.*		§ 13 odst. g)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Řízení změn						
Přezkoumávat možné dopady změn.			§ 11 odst.1 a)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Určovat významné změny.			§ 11 odst.1 b)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Dokumentovat řízení významných změn.			§ 11 odst.2 a)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Provádět analýzu rizik.	*U významných změn.*		§ 11 odst.2 b)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Přijímat opatření za účelem snížení všech nepříznivých dopadů významných změn.			§ 11 odst.2 c)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Aktualizovat bezpečnostní politiku a dokumentaci.	*U významných změn.*		§ 11 odst.2 d)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zajistit testování významných změn.			§ 11 odst.2 e)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zajistit možnost navrácení do původního stavu.	*U významných změn.*		§ 11 odst.2 f)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Rozhodovat o penetračním testování nebo testování zranitelností.	*Rozhoduje na základě výsledků analýzy rizik.*		§ 11 odst.3	X		
Řízení aktiv a rizik						
Řízení aktiv						
Stanovit metodiku pro identifikaci aktiv.			§ 4 odst.1 a)	X		
Stanovit metodiku pro hodnocení aktiv.	*V rozsahu alespoň dle přílohy č.1 VyKB.*		§ 4 odst.1 b)	X		
Identifikovat a evidovat aktiva.			§ 4 odst.1 c)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Určit a evidovat garanty aktiv.			§ 4 odst.1 d)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Hodnotit a evidovat primární aktiva z hlediska důvěrnosti, integrity a dostupnosti.	*Zařadit tato aktiva dle stanovené metodiky pro hodnocení aktiv.*		§ 4 odst.1 e)	X		
Určit a evidovat vazby mezi primárními a podpůrnými aktivy.	*Hodnotit důsledky jejich vzájemné závilosti.*		§ 4 odst.1 f)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Hodnotit podpůrná aktiva.	*Zohlednit vzájemné závilost dle § 4 odst.1 f)*		§ 4 odst.1 g)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Stanovit a zavádět pravidla ochrany pro jednotlivé úrovně aktiv.	*Dle hodnocení aktiv.*		§ 4 odst.1 h)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Stanovit přípustné způsoby používání aktiv a pravidla pro manipulaci s aktivy.	*Včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv.*		§ 4 odst.1 i)	X		
Určit způsob likvidace dat, provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat.	*S ohledem na úroveň aktiv a přílohu č.4 VyKB.*		§ 4 odst.1 j)	X		
Posoudit rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství.	*U primárních aktiv.*		§ 4 odst.2 a)	X		
Posoudit rozsah dotčených právních povinností a jiných závazků.	*U primárních aktiv.*		§ 4 odst.2 b)	X		
Posoudit rozsah narušení vnitřních řídích a kontrolních činností.	*U primárních aktiv.*		§ 4 odst.2 c)	X		
Posoudit poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty.	*U primárních aktiv.*		§ 4 odst.2 d)	X		
Posoudit dopady na poskytování důležitých služeb.	*U primárních aktiv.*		§ 4 odst.2 e)	X		
Posoudit rozsah narušení běžných činností.	*U primárních aktiv.*		§ 4 odst.2 f)	X		
Posoudit dopady na zachování dobrého jména nebo ochranu dobré pověsti.	*U primárních aktiv.*		§ 4 odst.2 g)	X		
Posoudit dopady na bezpečnost a zdraví osob.	*U primárních aktiv.*		§ 4 odst.2 h)	X		
Posoudit dopady na mezinárodní vztahy.	*U primárních aktiv.*		§ 4 odst.2 i)	X		
Posoudit dopady na uživatele informačního a komunikačního systému.	*U primárních aktiv.*		§ 4 odst.2 j)	X		

Řízení rizik						
Stanovit metodiku pro hodnocení rizik.	*Včetně stanovení kritérií pro akceptovatelnost rizik.*		§ 5 odst.1 a)	X		
S ohledem na aktiva identifikovat relevantní hrozby a zranitelnosti.	*Zvažovat kategorie hrozeb a zranitelností uvedené v příloze č. 3 VyKB.*		§ 5 odst.1 b)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Provádět hodnocení rizik.	*V pravidelných intervalech (osoba uvedené v § 3 písm. c), d) a f) zákona alespoň jednou ročně a osoba uvedená v § 3 písm. e) zákona alespoň jednou za tři roky) a při významných změnách.*		§ 5 odst.1 c)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Při hodnocení rizik zohlednit relevantní hrozby a zranitelnosti a posoudit možné dopady na aktiva.	*Alespoň v rozsahu uvedeném v příloze č.2 VyKB.*		§ 5 odst.1 d)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zpracovat zprávu o hodnocení rizik.			§ 5 odst.1 e)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zpracovat na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti.	*Musí obsahovat přehled bezpečnostních opatření požadovaných touto vyhláškou (aplikovných i neaplikovaných).*		§ 5 odst.1 f)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zpracovat a zavést plán zvládání rizik.	*Musí obsahovat cíle a přínosy bezpečnostních opatření pro zvládání jednotlivých rizik, určení osoby zajišťující prosazování bezpečnostní opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení, popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a způsob jejich realizace.*		§ 5 odst.1 g)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zohleďnovat některé atributy při hodnocení rizik v plánu zvládání rizik.	*Atributy: významné změny, změny rozsahu ISMS, opatření podle § 11 zákona, KBI včetně již řešených.*		§ 5 odst.1 h)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zavádět bezpečnostní opatření v souladu s plánem zvládání rizik.			§ 5 odst.1 i)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Řízení provozu a komunikací						
Řízení provozu a komunikací						
Stanovit práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role.			§ 10 odst. 1 a)	X		
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		
Stanovit pravidla a postupy pro sledování KBU a opatření pro ochranu přístupu k záznamům o těchto událostech.			§ 10 odst. 1 c)	X		
Stanovit pravidla a postupy pro ochranu před škodlivým kódem.			§ 10 odst. 1 d)	X		
Stanovit pravidla a postupy pro řízení technických zranitelností.			§ 10 odst. 1 e)	X		
Zajistit spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory.			§ 10 odst. 1 f)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Stanovit postupy řízení a schvalování provozních změn.			§ 10 odst. 1 g)	X		
Stanovit pravidla a postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.			§ 10 odst. 1 h)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Stanovit pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu.			§ 10 odst. 1 i)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Stanovit pravidla a postupy pro instalaci technických aktiv.			§ 10 odst. 1 j)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Stanovit provádění pravidelného zálohování a kontroly použitelnosti provedených záloh.			§ 10 odst. 1 k)	X		
Stanovit pravidla a postupy pro zajištění bezpečnosti síťových služeb.			§ 10 odst. 1 l)	X		
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		
Řídit přístup na základě skupin a rolí.			§ 12 odst. 2 a)	X		
Přídělit všem uživatelům a administrátorům přístupová práva a oprávnění a jedinečný identifikátor.			§ 12 odst. 2 b)	X		
Řídit identifikátory, přístupová práva, oprávnění aplikací a technických účtů.			§ 12 odst. 2 c)	X		
Zavádět bezpečnostní opatření pro řízení přístupu k prostředkům informačního a komunikačního systému.			§ 12 odst. 2 d)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zavádět bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení a jiných technických zařízení, popřípadě i bezpečnostní opatření spojená s využitím technických zařízení, která poviná osoba nemá ve správě.			§ 12 odst. 2 e)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Omezit přidělování privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce.			§ 12 odst. 2 f)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Omezit a kontrolovat používání programových prostředků, které mohou být schopné překonat systémové nebo aplikační kontroly.			§ 12 odst. 2 g)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Přidělovat a odebírat přístupová oprávnění v souladu s politikou řízení přístupu.			§ 12 odst. 2 h)	X		
Provádět pravidelné přezkoumání nastavení veškerých přístupových oprávnění včetně rozdělení do přístupových skupin a rolí.			§ 12 odst. 2 i)	X		
Využívat nástroj pro správu a ověřování identity a nástroj pro řízení oprávnění.			§ 12 odst. 2 j)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění

Prosazovat, aby uživatelé používali privátních autentizačních informací a dodržovali stanovené postupy.			§ 12 odst. 2 k)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zajistit odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.			§ 12 odst. 2 l)	X		
Zajistit odebrání nebo změnu přístupových oprávnění při ukončení nebo změně smluvního vztahu.			§ 12 odst. 2 m)	X		
Dokumentovat přidělování a odebírání přístupových oprávnění.			§ 12 odst. 2 n)	X		
Fyzická bezpečnost						
Předcházet poškození, krádeži nebo zneužití aktiv nebo porušení poskytování služeb informačního a komunikačního systému.			§ 17 odst. a)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
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	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Přijímat nezbytná opatření a uplatňovat prostředky fyzické bezpečnosti u fyzického bezpečnostního perimetru.	*Prostředky k zamezení neoprávněného vstupu, k zamezení poškození a neoprávněným zásahům a pro zajištění ochrany na úrovni a v rámci objektů.*		§ 17 odst. c)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Bezpečnost komunikační sítě						
Zajistit segmentaci komunikační sítě.			§ 18 odst. a)	X		
Zajistit řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě.			§ 18 odst. b)	X		
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		
Aktivně blokovat nežádoucí komunikaci.			§ 18 odst. d)	X		
Pro zajištění segmentace sítě a pro řízení komunikace mezi jejími segmenty využívat nástroj, který zajistí ochranu integrity sítě.			§ 18 odst. e)	X		
Správa o ověřování identit						
Používat nástroj pro správu a ověření identit uživatelů, administrátorů a aplikací komunikačního a informačního systému.			§ 19 odst.1	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Využívat autentizační mechanismus.	*Vícefaktorová autentizace.*			X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Ochrana před škodlivým kódem						
S ohledem na důležitost aktiv zajišťovat použití nástroje pro nepřetržitou automatickou ochranu.	*Ochrana koncových stanic, mobilních zařízení, serverů, datových úložišť a výměnných datových nosičů, komunikační sítě a prvků komunikační sítě a obdobných zařízení.*		§ 21 odst.1 a)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Monitorovat a řídit používání výměnných zařízení a datových nosičů.			§ 21 odst.1 b)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Řídit automatické spouštění obsahu výměnných zařízení a datových nosičů.			§ 21 odst.1 c)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Řídit oprávnění ke spuštění kódu.			§ 21 odst.1 d)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Provádět pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem.			§ 21 odst.1 e)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Kryptografické prostředky						
Používat aktuálně odolné kryptografické algoritmy a kryptografické klíče.			§ 26 odst. a)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Používat systém správy klíčů a certifikátů.	*Zajistit generování, distribuci, ukládání změny, omezení platnosti, zneplatnění certifikátů a likvidaci klíčů a umožnit kontrolu a audit.*		§ 26 odst. b)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Prosazovat bezpečné nakládání s kryptografickými prostředky.			§ 26 odst. c)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zohledňovat doporučení v oblasti kryptografických prostředků vydaných Úřadem.			§ 26 odst. d)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Bezpečnost lidských zdrojů						
Stanovit plán rozvoje bezpečnostního povědomí.	*Obsahuje formu, obsah a rozsah poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice a obsahuje formu, obsah a rozsah potřebných teoretických i praktických školení uživatelů, administrátorů a osob zastávajících bezpečnostní role.*		§ 9 odst. 1 a)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Určit osoby zodpovědné za realizaci jednotlivých činností.			§ 9 odst. 1 b)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
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	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zajistit pravidelná odborná školení pro osoby zastávající bezpečnostní role.			§ 9 odst. 1 d)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zajistit pravidelná školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní.			§ 9 odst. 1 e)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zajistit kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.			§ 9 odst. 1 f)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění

Zajistit předání odpovědnostní v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role.			§ 9 odst. 1 g)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Hodnotit účinnost plánu rozvoje bezpečnostního povědomí.			§ 9 odst. 1 h)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Určit pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel.			§ 9 odst. 1 i)	X		Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Vést evidence školení a osob, které je absolvovaly.			§ 9 odst. 2	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
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		
Ověřit a kontrolovat přenášená data na perimetru komunikační sítě.			§ 23 odst.1 b)	X		
Blokovat nežádoucí komunikaci.			§ 23 odst.1 c)	X		
Zajistit detekci KBU s ohledem na důležitost aktiv v rámci jednotlivých míst.	*Koncové stanice, mobilní zařízení, servery, datová úložiště a výměnné datové nosiče, síťové aktivní prvky a obdobná aktiva.*		§ 23 odst.2	X		
Sběr a vyhodnocení kybernetických bezpečnostní událostí						
Sbírat a vyhodnocovat události zaznamenané dle § 22 a § 23 VyKB.			§ 24 odst. a)	X		
Vyhledávat a seskupovat související záznamy.			§ 24 odst. b)	X		
Poskytovat informace pro určené bezpečnostní role o detekovaných KBU.			§ 24 odst. c)	X		
Vyhodnocovat KBU s cílem identifikace KBU.	*Včetně všasného varování určených bezpečnostních rolí.*		§ 24 odst. d)	X		
Omezit případy nesprávného vyhodnocení událostí pravidelnou aktualizací pravidel.	*Pravidla pro vyhodnocování KBU a pro včasné varování.*		§ 24 odst. e)	X		
Využívat informace získané nástrojem pro sběr a vyhodnocení KBU pro optimální nastavení bezpečnostních opatření informačního a komunikačního systému.			§ 24 odst. f)	X		
Řízení kontinuity činností						
Stanovit práva a povinnosti administrátorů a osob zastávajících bezpečnostní role.	*V rámci řízení kontinuity činností.*		§ 15 odst. a)	X		
Pomocí hodnocení rizik a analýzy dopadů vyhodnotit a dokumentovat možné dopady KBI a posoudit možná rizika související s ohrožením kontinuity činností.			§ 15 odst. b)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Na základě výstupů hodnotit rizika a analýzy dopadů a stanovit cíle řízení kontinuity činností.	*Forma určení: minimální úroveň poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního a komunikačního systému; doba obnovení chodu během které bude po KBI obnovena minimální úroveň poskytovaných služeb informačního a komunikačního systému; bod obnovení dat jako časové období, za které musí být zpětně obnovena data po KBI nebo po selhání.*		§ 15 odst. c)	X		
Stanovit politiku řízení kontinuity činností.	*Musí obsahovat naplnění cílů.*		§ 15 odst. d)	X		
Vypracovat, aktualizovat a pravidelně testovat plány kontinuity činností a havarijní plány související s provozováním informačního a komunikačního systému.			§ 15 odst. e)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Realizovat opatření pro zvýšení odolnosti informačního a komunikačního systému vůči KBI a omezením dostupnosti.			§ 15 odst. f)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zvládání kybernetických bezpečnostních událostí a incidentů						
Zavést proces detekce a vyhodnocování KBU a zvládání KBI			§ 14 odst.1 a)	X		
Přidělení odpovědnosti a stanovení postupů.	*Postupy a odpovědnosti pro detekci a vyhodnocování KBI a KBI, pro koordinaci a zvládání KBI.*		§ 14 odst.1 b)	X		
Definovat a aplikovat postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu KBI.			§ 14 odst.1 c)	X		
Zajistit detekci KBU.			§ 14 odst.1 d)	X		
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	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zajistit posuzování KBU.	*Rozhodovat o jejich klasifikaci.*		§ 14 odst.1 g)	X		
Zajistit zvládání KBI.			§ 14 odst.1 h)	X		
Přijímat opatření pro odvrácení a zmírnění dopadu KBI.			§ 14 odst.1 i)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Hlásit KBI.			§ 14 odst.1 j)	X		
Vést záznamy o KBI a jejich zvládání.			§ 14 odst.1 k)	X		
Prošetřit a určit příčiny KBI.			§ 14 odst.1 l)	X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Vyhodnotit účinnost řešení KBI.	*Stanovit nutná bezpečnostní opatření nebo aktualizovat stávající.*		§ 14 odst.1 m)	X		
Audit kybernetické bezpečnosti						
Provádět a dokumentovat dodržování bezpečnostní politiky.	*Včetně přezkoumání technické shody. Výsledky auditu zohlednit v plánu zvládání rizik a v plánu rozvoje bezpečnostního povědomí.*		§ 16 odst.1 a)	X		
Posuzovat soulad bezpečnostních opatření s nejlepší praxí, právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu a komunikačnímu systému.	*Určit případná nápravná opatření.*		§ 16 odst.1 b)	X		
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	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění

Zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro informační a komunikační systém a tyto požadavky zahrnout do uzavírané smlouvy.	*Definovat a uplatňovat požadavky do smluv s dodavateli / subdodavateli*	§ 4 odst.4		X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Zajistit si ve smlouvě s dodavatelem cloud computingu dodržování bezpečnostních pravidel pro poskytování služeb cloud computingu stanovených Úřadem.	*Musí mít k dispozici na základě své žádosti bez zbytečného odkladu informace a data, která pro ně poskytovatel služeb cloud computingu uchovává.*	§ 4 odst.5		X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Informovat provozovatele systému o tom, že se orgán nebo osoba stala správcem informačního nebo komunikačního systému kritické informační infrastruktury nebo správcem významného informačního systému a o tom, že se tento provozovatel stal orgánem nebo osobou dle § 3 písm. c), d) a e).		§ 4a odst.1		X		
Informovat subjekt zajišťující síť elektronických komunikací, ke které je předmětný informační nebo komunikační systém kritické informační infrasktruktury připojen, že se orgán nebo osoba stala správcem nebo provozovatelem informačních nebo komunikačních systému kritické informační infrastruktury a o tom, že se tento subjekt stal orgánem nebo osobou dle § 3 písm. c), d) a e).		§ 4a odst.2		X		
Pokud se orgán nebo osoba stala provozovatelem základní služby, ale není správcem nebo provozovatelem informačních systémů základní služby, je povinna správce nebo provozovatele tohoto informačního systému informovat o svém určení a o tom, že se dotčený správce nebo provozovatel stal orgánem dle § 3 písm. f).		§ 4a odst.3		X		
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		
Hlásit KBI ve významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému.	*Bezodkladně po detekci.*	§ 8 odst.1		X		
Hlásit KBI provozovateli národního CERT.		§ 8 odst.3		X		
Hlásit KBI Úřadu.		§ 8 odst.4		X		
Opatření						
Provádět reaktivní opatření.		§ 11 odst.3		X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
Oznámit Úřadu reaktivní opatření a jeho výsledek.		§ 13 odst.4		X		
Dokumentace						
1. Bezpečnostní politika				X		
1.1. Politika systému řízení bezpečnosti informací				X		
1.2. Politika řízení aktiv				X		
1.3. Politika organizační bezpečnosti				X		
1.4. Politika řízení dodavatelů				X		
1.5. Politika bezpečnosti lidských zdrojů				X		
1.6 Politika řízení provozu a komunikací				X		
1.7. Politika řízení přístupu				X		
1.8. Politika bezpečného chování uživatelů				X		
1.9. Politika zálohování a obnovy a dlouhodobého ukládání				X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
1.10. Politika bezpečného předávání a výměny informací				X		
1.11. Politika řízení technických zranitelností				X		
1.12. Politika bezpečného používání mobilních zařízení				X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
1.13. Politika akvizice, vývoje a údržby				X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
1.14. Politika ochrany osobních údajů				X		
1.15. Politika fyzické bezpečnosti				X		
1.16. Politika bezpečnosti komunikační sítě				X		
1.17. Politika ochrany před škodlivým kódem				X		
1.18. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí				X		
1.19. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí				X		
1.20. Politika bezpečného používání kryptografické ochrany				X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
1.21. Politika řízení změn				X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
1.22. Politika zvládání kybernetických bezpečnostních incidentů				X		
1.23. Politika řízení kontinuity činností				X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
2.1. Zpráva z auditu kybernetické bezpečnosti				X		
2.2. Zpráva z přezkoumání systému řízení bezpečnosti informací				X		
2.3. Metodika pro identifikaci a hodnocení aktiv a pro hodnocení rizik				X		
2.4. Zpráva o hodnocení aktiv a rizik	*Analýza rizik*			X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
2.5. Prohlášení o aplikovatelnosti	*Analýza rizik*			X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
2.6. Plán zvládání rizik				X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění

2.7. Plán rozvoje bezpečnostního povědomí				X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
2.8. Evidence změn				X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění
2.9. Hlášené kontaktní údaje				X		
2.10. Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků				X		
Příl. č. 7 Řízení dodavatelů - bezpečnostní opatření pro smluvní vztahy	*k) specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností).*			X	X	Spolupráce Poskytovatele v rámci dodávaného Předmětu plnění