Příloha č. 11 ke Smlouvě č. j.: MV-101487-60/VZ-2022

Bezpečnostní opatření pro smluvní vztahy

1. ÚVOD

Tato příloha Smlouvy popisuje bezpečnostní požadavky projektu „Informační systém sociálního zabezpečení (DP-3)“ zejména pro naplnění požadavků vyplývajících ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZoKB“), a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti (dále jen „VyKB“), pro významný informační systém resortu MV.

2. BEZPEČNOSTNÍ POŽADAVKY

2.1. Účel

1. Tato příloha Smlouvy stanoví způsoby a úrovně realizace bezpečnostních opatření pro Zhotovitele a určuje vzájemný vztah odpovědnosti za zavedení a kontrolu bezpečnostních opatření mezi Objednatelem a Zhotovitelem. Požadavky na Zhotovitele jsou definovány dle platné právní úpravy, především pak dle ZoKB, VyKB a zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (dále jen „ZISVS“).
2. Smluvní strany se dohodly, že pokud to bude potřebné ke splnění požadavků ZoKB, VyKB, ZISVS, či souvisejících právních předpisů z oblasti bezpečnosti informací, uzavřou bez zbytečného odkladu po výzvě kterékoli smluvní strany písemný dodatek Smlouvy zohledňující takové požadavky.

2.2. Obecné bezpečnostně provozní požadavky

Zhotovitel se při poskytování plnění pro Objednatele zavazuje plnit následující povinnosti:

1. postupovat v souladu s účinnými právními předpisy, zejména pak požadavky vyplývajícími pro Zhotovitele, jakožto budoucího významného dodavatele významného informačního systému, ze ZoKB, VyKB a ZISVS a reflektovat případné novely dotčených právních předpisů či novou právní úpravu, a bezpečnostními politikami stanovenými systémem řízení bezpečnosti informací (ISMS) Objednatele dle specifikace předmětu veřejné zakázky;
2. nejpozději do tří pracovních dnů po dni účinnosti Smlouvy jmenovat ze členů realizačního týmu za Zhotovitele zodpovědnou kontaktní osobu pro potřeby zajištění plnění bezpečnostních požadavků vyplývajících ze Smlouvy a této přílohy a související komunikace mezi smluvními stranami (dále také jen „Kontaktní osoba pro bezpečnost na straně Zhotovitele“). Kontaktní osobu pro bezpečnost na straně Zhotovitele sdělí písemně Objednateli v téže lhůtě;

3. zajistit, aby Kontaktní osoba pro bezpečnost na straně Zhotovitele nejpozději do 30 dnů od uzavření Smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování plnění této Smlouvy za stranu Zhotovitele a/nebo jeho poddodavatelé byli prokazatelně seznámeni s těmito Bezpečnostními požadavky;
4. minimálně 1x ročně provádět identifikaci a hodnocení aktiv a rizik významného informačního systému, která je součástí dodávaného řešení a na základě výsledků navrhovat a předkládat Objednateli ke schválení opatření na minimalizaci nebo odstranění zjištěných rizik. Opatření musí být navrhována a konsolidována s přihlédnutím k výsledkům posuzování rizik i z hlediska dopadu na práva a svobody subjektů údajů.
5. dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů předaných Zhotoviteli Objednatelem, k jejímuž dodržování se Zhotovitel zavázal, pokud byl Zhotovitel s takovými dokumenty nebo jejich částmi seznámen, a to bez ohledu na způsob, jakým byl s takovou dokumentací Objednatele seznámen (např. školením, protokolárním předáním příslušné dokumentace Zhotoviteli, elektronickým předáním prostřednictvím e-mailu či datovou schránkou, zřízením přístupu Zhotoviteli na sdílené úložiště aj.); vymezení relevantní části centrální dokumentace ISMS, která byla předána Zhotoviteli, je uveden v Příloze č. 12 Smlouvy.
6. rozvíjet bezpečnostní povědomí svých zaměstnanců a příp. dalších osob, které se podílejí na plnění Smlouvy a průběžně je seznamovat s prováděnými nebo plánovanými změnami. Zaměstnanci a další osoby na straně Zhotovitele podílející se na plnění Smlouvy musí být prokazatelně seznámeni s platnými předpisy a bezpečnostními požadavky Objednatele, a to ještě před zahájením jakékoli činnosti ze strany těchto osob pro Objednatele v souvislosti s plněním této Smlouvy;
7. zaznamenávat a na vyžádání Objednateli poskytnout veškeré podstatné okolnosti související s poskytovaným předmětem plnění dle Smlouvy (technické záznamy, organizační záznamy o školení, pověření apod.);
8. přidělovat svým jednotlivým pracovníkům oprávnění k výkonu činností a přísně při tom dodržovat bezpečnostní zásadu tzv. „potřeba vědět“ (need-to-know principle), tedy zejména dbát o to, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele;
9. garantovat dostupnost, důvěrnost plnění a integritu předávaných dat s tím, že dodávané služby musí být v souladu s uzavřeným smluvním vztahem provozně monitorovány a vyhodnocovány;
10. průběžně dokumentovat, kontrolovat a vyhodnocovat oprávněnost přístupu, jak fyzického, tak i logického, u všech osob na straně Zhotovitele, které přistupují k předmětu plnění dle této Smlouvy;
11. zavést opatření pro ochranu zálohy dat vztahujících se k plnění Smlouvy a pravidelně (alespoň 1x za čtvrtletí, vždy ale s minimálně dvouměsíčním odstupem) testovat funkčnost těchto záloh;
12. průběžně detekovat, minimálně však jednou za 3 měsíce, technické zranitelnosti a konfigurační nesoulady předmětu plnění Smlouvy a o zjištěných skutečnostech bez zbytečného odkladu informovat Objednatele. Detekované technické zranitelnosti musí být vyhodnoceny s ohledem na související riziko a musí podle povahy předmětu plnění dojít

k nápravným opatřením ze strany Zhotovitele. Nápravná opatření musí být schválena Objednatelem;

13. zajistit rozhraní pro napojení na dohledová centra Objednatele a součinnost při zvládání kybernetických bezpečnostních událostí a incidentů;
14. uchovávat data o provozu (provozní a lokalizační údaje) v souladu s požadavky účinné legislativy ČR a dodržovat požadavky VyKB na obsah provozních událostí.

2.3. Oprávnění užívat data

1. Zhotovitel je při poskytování plnění pro Objednatele oprávněn nakládat s daty předanými Zhotoviteli Objednatelem výhradně za účelem plnění předmětu Smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy.
2. Zhotovitel se při poskytování plnění pro Objednatele zavazuje nakládat s daty pouze v souladu se Smlouvou a příslušnými právními předpisy, zejména ZoKB, VyKB a dalšími souvisejícími právními předpisy.

2.4. Kontrola souladu s požadavky bezpečnosti

1. Zhotovitel je srozuměn s prováděním hodnocení rizik, kontrolou a auditem zavedených bezpečnostních opatření ze strany Objednatele v souvislosti s poskytovanou službou Zhotovitelem.
2. Hodnocení, kontrola a audit probíhají v intervalech stanovených Objednatelem nebo v případě vzniku kybernetického bezpečnostního incidentu v rámci poskytované služby nebo v případě, že se vznik bezpečnostního incidentu jeví jako pravděpodobný. Kontrola nebo audit mohou být provedeny v prostorách Zhotovitele nebo jeho poddodavatele a Zhotovitel má povinnost tyto kontroly a audity Objednateli či Objednatelem pověřené osobě umožnit či možnost jejich provedení v prostorách poddodavatele zajistit, přispět k nim a poskytnout Objednateli či Objednatelem pověřené osobě k jejich provedení maximální možnou součinnost, kterou lze po Zhotoviteli rozumně požadovat. Počet a frekvence kontrol ani auditů nejsou nijak omezeny.
3. Zhotovitel je povinen po zavedení opatření provést také vlastní hodnocení rizik a kontrolu zavedených bezpečnostních opatření. Tato kontrola probíhá v pravidelných intervalech stanovených Objednatelem, na žádost Objednatele nebo v případě vzniku kybernetického bezpečnostního incidentu v rámci poskytované služby nebo v případě, že se vznik bezpečnostního incidentu jeví jako pravděpodobný. O výsledku kontroly podá Zhotovitel Objednateli bez zbytečného odkladu písemnou kontrolní zprávu.

2.5. Řetězení a řízení dodavatelů

Zhotovitel se při poskytování plnění pro Objednatele zavazuje plnit následující povinnosti:

1. Zhotovitel nezapojí do poskytování plnění dle této Smlouvy žádného dalšího poddodavatele bez předchozího konkrétního písemného povolení Objednatele;

2. Zhotovitel se zavazuje, že se bude řídit požadavky Objednatele na řízení bezpečnosti informací a poskytne Objednateli veškerou nezbytnou součinnost v otázkách řízení bezpečnosti informací a pokud využívá při poskytování plnění poddodavatele, zajistí, že bude Objednateli poskytnuta veškerá nezbytná součinnost v otázkách řízení bezpečnosti informací také od těchto poddodavatelů;
3. Zhotovitel je povinen předat Objednateli kontaktní údaje všech osob dodávajících systémovou a technickou podporu pro řešení;
4. Pokud Zhotovitel využívá při poskytování plnění poddodavatele, zavazuje se, že budou dodržovat bezpečnostní požadavky vč. požadavků na ochranu osobních údajů vyplývající z této Smlouvy. Zhotovitel se zavazuje bezodkladně doložit Objednateli na základě jeho výzvy smluvní dokumenty se svými poddodavateli, ze kterých bude vyplývat závazek poddodavatele poskytovat plnění v souladu s bezpečnostními požadavky vyplývajícími z této Smlouvy;
5. Zhotovitel odpovídá za to, že jeho poddodavatelé nebudou jednat v rozporu s bezpečnostními požadavky vyplývajícími z této Smlouvy; v případě, že dojde k nedodržení těchto požadavků ze strany poddodavatele Zhotovitele, považuje se každé takové nedodržení požadavků za porušení povinnosti Zhotovitele dle této Smlouvy.

2.6. Povinnosti v řízení změn dle ZoKB a VyKB

1. Zhotovitel se zavazuje v rozsahu předmětu plnění aktivně podílet na splnění povinností v oblasti řízení změn dle ZoKB a VyKB, zejména při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu.
2. Zhotovitel se minimálně zavazuje v rozsahu předmětu plnění na své straně přiměřeně reagovat na změny a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.
3. Zhotovitel se zavazuje aktivně spolupracovat při testování významné změny.

2.7. Zvládání bezpečnostních událostí a incidentů

Zhotovitel se při poskytování plnění pro Objednatele zavazuje, že:

1. stanoví činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních událostí a incidentů, podle takto stanovených a popsaných pravidel bude postupovat, a bude hlásit všechny bezpečnostní události a incidenty neprodleně po jejich detekci Objednateli prostřednictvím ohlašovacích kanálů Objednatele, v případech, kdy situace nestrpí odklad telefonicky. Dále se zavazuje vyhodnotit informace o bezpečnostních událostech a incidentech a o těchto informacích, vzniklých bezpečnostních incidentech, vč. krátkodobých a dlouhodobých nápravných opatřeních nad všemi částmi řešení, které jsou ve správě Zhotovitele, a rizicích souvisejících s ohrožením kontinuity činností vést záznamy a tyto uchovat pro jejich budoucí použití s ohledem na požadavky Objednatele a legislativy ČR. Nastavená pravidla a postupy podléhají schválení Objednatelem;

2. nastavená pravidla pro zvládání bezpečnostních incidentů budou respektovat požadavek na legalitu zajištění stop, tj. jejich původ a oprávněnost jejich získaní musí být v souladu s platnými zákony a standardy tak, aby bylo možné jejich následné využití v rámci forenzní analýzy a eventuální použití jako důkazní materiál;
3. navrhne řešení tak, aby byl systém detekce a zvládání bezpečnostních událostí a incidentů začleněn do procesů a systémů a realizuje opatření pro zvýšení odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti;
4. zajistí rozhraní pro napojení na dohledová centra Objednatele pro zvládání kybernetických bezpečnostních událostí a incidentů a zajistí součinnost a bude se řídit jeho pokyny;
5. provede analýzu příčin bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že Zhotovitel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

2.8. Informační povinnost a povinnosti při výměně informací

1. Zhotovitel se během poskytování plnění pro Objednatele zavazuje Objednatele informovat o:
   a) způsobu řízení rizik, zbytkových rizicích souvisejících s plněním Smlouvy a bez zbytečného odkladu také o změnách ve způsobu řízení rizik;
   b) významné změně ovládání Zhotovitele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných Zhotovitelem k plnění na základě smluvního vztahu s Objednatelem.
2. Zhotovitel se během poskytování plnění pro Objednatele zavazuje dostatečně zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost před hrozbami v kybernetické bezpečnosti v souladu s ZoKB a VyKB.

2.9. Specifikace podmínek pro řízení kontinuity činností a zálohování a obnovu dat z pohledu ZoKB a VyKB

1. Zhotovitel se zavazuje zpracovat plán řízení KBI a plán kontinuity a obnovy činností souvisejících s provozem řešení a všech jeho komponent na základě Zhotovitelem zpracovaného zhodnocení a výsledků z analýzy dopadů (Business Impact Analysis), která musí být schválena Objednatelem.
2. Zhotovitel se zavazuje dodržovat požadavky Objednatele na řízení kontinuity činností v souladu s ZoKB, VyKB a ustanoveními bezpečnostní politik, metodik a postupů předaných Zhotoviteli Objednatelem.
3. Zhotovitel vypracuje a předá Objednateli metodiku zálohování a obnovy dat (ve smyslu primárních aktiv) i systémů (resp. technických aktiv) ve formě zálohovacího plánu, testovacího scénáře obnovy dat, systému evidence, zajištění integrity a autenticity zálohovacího média. Záloha jako taková musí být šifrována. Zhotovitel jako součást

dodávky dále dodá a nasadí odpovídající technologické řešení, na kterém bude záloha a obnova dat prováděna. Toto řešení musí být nasazeno v primární i záložní lokalitě.

4. Plán řízení KBI, plán kontinuity a obnovy činností a metodika zálohování a obnovy dat i systémů musí být zpracovány nejpozději v rámci etapy 6 Díla.

2.10. Bezpečnost lidských zdrojů

1. Zhotovitel připraví poučení a zajistí poučení všech stran podílejících se na poskytování předmětu plnění dle Smlouvy o bezpečnostních pravidlech, jež se musí v průběhu dodávky dodržovat a zajistí jejich dodržování nasazením kontrolních a vynucovacích mechanismů. Rozsah poučení podléhá schválení Objednatele.
2. Zhotovitel se zaváže zajistit dostatečnou míru zastupitelnosti pro technické aspekty řešení (zajištění kontinuity dodávky, zastupitelnost pracovníků, zejména Kontaktní osoba pro bezpečnost na straně Zhotovitele).

2.11. Požadavky na systémovou a provozní bezpečnostní dokumentaci

1. Nedílnou součástí poskytovaného plnění je zdokumentování všech bezpečnostních nastavení, funkcí a mechanismů formou zpracování bezpečnostní dokumentace a dále také zpracování provozní dokumentace. Tato dokumentace musí být v souladu se ZoKB a VyKB.
2. V rámci poskytovaného plnění se Zhotovitel zavazuje Objednateli předat následující dokumentaci k řešení dle platné legislativy a dle požadavků Objednatele:
   a) Bezpečnostní dokumentace významného informačního systému:
      i. bezpečnostní politika,
      ii. bezpečnostní směrnice pro činnost bezpečnostního správce systému,
      iii. bezpečnostní a provozní postupy definující požadavky, procesní pravidla, role a odpovědnost v rámci jednotlivých procesů v rámci celého životního cyklu IS (od zajištění vývoje a rozvoje nových funkčností IS, následného předání do provozu, provozování a správy IS, nebo zařízení v produkci až po jeho vyřazení z používání).
   b) Systémová příručka obsahující:
      i. popis funkcí, včetně bezpečnostních, které používá správce systému pro provádění určených činností v informačním systému veřejné správy a návod na používání těchto funkcí,
      ii. parametry kvality vycházejí z požadavků na kvalitu,
      iii. podrobný popis IS nebo odkaz na dokument, ve kterém je popis uveden a který je Objednateli dostupný,
      iv. popis jednotlivých činností vykonávaných při správě IS, včetně činností definovaných pro role, určení fyzických osob, které tyto činnosti vykonávají a oprávnění nezbytných pro výkon těchto činností,

v. definování uživatelů nebo skupin uživatelů a jejich oprávnění a povinnosti při využívání IS.

c) Uživatelská příručka obsahující:

i. popis funkcí, včetně bezpečnostních, které používá uživatel pro svou činnost v IS a návod na použití těchto funkcí,

ii. vymezení oprávnění a povinností uživatelů ve vztahu k IS.

d) Dokumentace k integraci řešení, a to včetně identifikovaných datových toků, protokolů, architektonického nákresu komponent a jejich spolupráce, diagram logického a fyzického zapojení.

e) Další dokumentaci dle požadavku Objednatele.

f) Zhotovitel se v rámci poskytovaného plnění pro Objednatele zavazuje předat Objednateli také provozní dokumentaci v obdobném rozsahu dle předmětu a povahy Smlouvy:

i. dokumentaci strategie obnovy,

ii. dokumentaci skutečného provedení,

iii. dokumentaci obsahující popis autorizačního konceptu a oprávnění,

iv. dokumentaci obsahující zálohovací a archivační postupy,

v. dokumentaci obsahující instalační a konfigurační postupy,

vi. dokumentaci obsahující bezpečností nastavení související s předmětem plnění smlouvy;

dále jen souhrnně „**Bezpečnostní a provozní dokumentace**“.

3. Bezpečnostní a provozní dokumentace musí být vytvořena dle poskytnutých šablon v rámci etapy 6 Díla.

4. Bezpečnostní a provozní dokumentace uvedená výše bude Objednateli Zhotovitelem předána nad rámec případné jiné předávané dokumentace vymezené v této Smlouvě.

2.12. Fyzická ochrana a bezpečnost prostředí

1. Zhotovitel se zavazuje dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny komponenty technologických a komunikačních systémů, anebo datové nosiče (dále také jen „**Pracoviště**“).

2. Zhotovitel se zavazuje, že na Pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k předmětu plnění dle této Smlouvy.

2.13. Požadavky na Řízení přístupu

1. Zhotovitel bere na vědomí, že přístup k datům, informacím či zařízením souvisejícím s předmětem Smlouvy je možné povolit pouze konkrétním fyzickým osobám / zaměstnancům Zhotovitele / poddodavatele Zhotovitele zaevidované, a to na základě požadavku Zhotovitele na přístup.

2. Zhotovitel bere na vědomí, že přidělení oprávnění zaměstnanci Zhotovitele musí být řízeno zásadou tzv. „potřeba vědět“ (need-to-know principle) a není nárokové.
3. Zhotovitel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Zhotovitele nebo poddodavatele Zhotovitele.
4. Zhotovitel se zavazuje, že nebude instalovat a používat žádné nástroje, které nebyly předem písemně odsouhlaseny Objednatelem.
5. Zhotovitel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části technologického nebo komunikačního systému programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci technologického nebo komunikačního systému nebo nelegální získání dat a informací. Zhotovitel bere na vědomí, že přístup do interní sítě Objednatele a/nebo k technologickým a komunikačním systémům Objednatele bude realizován výhradně s využitím zařízení Objednatele.
6. Zhotovitel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě a/nebo technologického nebo komunikačního systému chránili autentizační prostředky a údaje k systémům Objednatele. Zhotovitel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako bezpečnostní incident ve smyslu příslušné řídící dokumentace a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu platí pro Zhotovitele, pokud byl s takovou řídící dokumentací Objednatele seznámen).
7. Zhotovitel bere na vědomí, že postup zvládání bezpečnostního incidentu či skutečnosti vzniklé v důsledku porušení Bezpečnostních požadavků nebude posuzována jako okolnost vylučující odpovědnost Zhotovitele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Zhotoviteli či jiné osobě ze strany Zhotovitele. Ostatní ustanovení ohledně odpovědnosti Zhotovitele za prodlení obsažená v Smlouvě nejsou tímto ustanovením dotčena.

2.14. Monitorování činností

1. Zhotovitel bere na vědomí, že veškerá aktivita Zhotovitele a jeho plnění realizované v rámci plnění předmětu Smlouvy nebo s ním úzce související budou Objednatelem průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na obsah Smlouvy a interních dokumentů Objednatele.
2. Zhotovitel se zavazuje, že bude průběžně monitorovat a zaznamenávat veškerou svoji aktivitu a plnění realizované v rámci plnění předmětu Smlouvy nebo s ním úzce související. Zhotovitel je povinen předkládat Objednateli záznamy/logy obsahující výsledky monitorování, úspěšná a neúspěšná přihlášení do ICT systému a záznamy o správě uživatelů prováděná na straně Zhotovitele, a to v pravidelných intervalech dle sjednaného harmonogramu, nebo kdykoli bez zbytečného odkladu po vyžádání ze strany Objednatele, a to po celou dobu trvání Smlouvy a i ve vztahu k jejímu ukončení.

2.15. Předání a převzetí plnění

1. Zhotovitel se zavazuje dodržovat Bezpečnostní požadavky i při předání a převzetí plnění dle této Smlouvy
2. Objednatel je oprávněn z důvodu nedodržení Bezpečnostních požadavků včetně požadavku na předání Bezpečnostní dokumentace odmítnout převzetí (části) plnění Smlouvy.

2.16. Likvidace dat

Zhotovitel se zavazuje plnit požadavky Objednatele v oblasti likvidace dat (ať už dat na papírových médiích, dat zpracovávaných elektronicky nebo prostřednictvím jakýchkoli dalších nosičů dat) dle přílohy č. 4 VyKB.

2.17. Sankce

Sankce za porušení povinností plynoucích z bezpečnostních opatření a ZoKB a VyKB jsou uvedeny v hlavním textu smlouvy.

2.18. Způsob distribuce dokumentů Objednateli

Zhotovitel má právo vyžádat si od Objednatele shora uvedené dokumenty vymezené v Příloze č. 12 Smlouvy, které mu budou předány na základě Dohody o zachování mlčenlivosti o důvěrných informacích (NDA).

Název	Popis	ZoKB	VyKB	Provádí		Poznámka
		§, odstavec	§, odstavec	Objenatel	Zhotovitel	
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	
Řídit rizika podle § 5 VyKB.			§ 3 odst. d)	X	X	
Vytvořit a schválit bezpečnostní politiku ISMS.	*Musí obsahovat zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti.*		§ 3 odst. e)	X	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	X	
Identifikovat a řídit významné změny.	*Podle § 11.*		§ 3 odst. h)	X	X	
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	
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	X	
Zajistit integraci ISMS do procesů povinné osoby.			§ 6 odst.1 b)	X	X	
Zajistit dostupnost zdrojů potřebných pro ISMS.			§ 6 odst.1 c)	X	X	
Informovat zaměstnance o významu ISMS a o významu dosažení shody s jeho požadavky se všemi dotčenými stranami.			§ 6 odst.1 d)	X	X	
Zajistit podporu k dosažení zamýšlených výstupů ISMS.			§ 6 odst.1 e)	X	X	
Vést zaměstnance k rozvíjení efektivity ISMS.			§ 6 odst.1 f)	X	X	
Prosazovat neustálé zlepšování ISMS.			§ 6 odst.1 g)	X	X	
Podporovat osoby zastávající bezpečnostní role při prosazování KB v oblastech jejich odpovědnosti.			§ 6 odst.1 h)	X	X	
Zajistit stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role.			§ 6 odst.1 i)	X	X	
Zajistit zachování mlčenlivosti administrátorů a osob zastávajících bezpečnostní role.			§ 6 odst.1 j)	X	X	
Zajistit pro osoby, které zastávají bezpečnostní role, příslušné pravomoci a zdroje.	*Včetně rozpočtových prostředků k naplňování jejich rolí.*		§ 6 odst.1 k)	X	X	
Zajistit testování plánu kontinuity činností, obnovy a procesů spojených se zvládáním KBI.			§ 6 odst.1 l)	X	X	
Určit složení VKB a bezpečnostní role a jejich práva a povinnosti související s ISMS.			§ 6 odst.2	X	X	
Určit osoby, které budou zastávat bezpečnostní role.	*MKB, architekt KB, auditor KB, garant aktiva.*		§ 6 odst.3	X		
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	
Řídit rizika spojené s dodavateli.			§ 8 odst.1 e)	X	X	
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	
Řídit významné změny podle § 11.	*V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému.*		§ 13 odst. b)	X	X	
Stanovit bezpečnostní požadavky.	*V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému.*		§ 13 odst. c)	X	X	
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	
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	
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	
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	
Řízení změn						
Přezkoumávat možné dopady změn.			§ 11 odst.1 a)	X	X	
Určovat významné změny.			§ 11 odst.1 b)	X	X	
Dokumentovat řízení významných změn.			§ 11 odst.2 a)	X	X	

Provádět analýzu rizik.	*U významných změn.*		§ 11 odst.2 b)	X	X	
Přijímat opatření za účelem snížení všech nepříznivých dopadů významných změn.			§ 11 odst.2 c)	X	X	
Aktualizovat bezpečnostní politiku a dokumentaci.	*U významných změn.*		§ 11 odst.2 d)	X	X	
Zajistit testování významných změn.			§ 11 odst.2 e)	X	X	
Zajistit možnost navrácení do původního stavu.	*U významných změn.*		§ 11 odst.2 f)	X	X	
Rozhodovat o penetračním testování nebo testování zranitelností.	*Rozhoduje na základě výsledků analýzy rizik.*			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	
Určit a evidovat garanty aktiv.			§ 4 odst.1 d)	X		
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	X	
Určit a evidovat vazby mezi primárními a podpůrnými aktivy.	*Hodnotit důsledky jejich vzájemné závilosti.*		§ 4 odst.1 f)	X	X	
Hodnotit podpůrná aktiva.	*Zohlednit vzájemné závilost dle § 4 odst.1 f)*		§ 4 odst.1 g)	X	X	
Stanovit a zavádět pravidla ochrany pro jednotlivé úrovně aktiv.	*Dle hodnocení aktiv.*		§ 4 odst.1 h)	X	X	
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	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	X	
Posoudit rozsah dotčených právních povinností a jiných závazků.	*U primárních aktiv.*		§ 4 odst.2 b)	X	X	
Posoudit rozsah narušení vnitřních řídích a kontrolních činností.	*U primárních aktiv.*		§ 4 odst.2 c)	X	X	
Posoudit poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty.	*U primárních aktiv.*		§ 4 odst.2 d)	X	X	
Posoudit dopady na poskytování důležitých služeb.	*U primárních aktiv.*		§ 4 odst.2 e)	X	X	
Posoudit rozsah narušení běžných činností.	*U primárních aktiv.*		§ 4 odst.2 f)	X	X	
Posoudit dopady na zachování dobrého jména nebo ochranu dobré pověsti.	*U primárních aktiv.*		§ 4 odst.2 g)	X	X	
Posoudit dopady na bezpečnost a zdraví osob.	*U primárních aktiv.*		§ 4 odst.2 h)	X	X	
Posoudit dopady na mezinárodní vztahy.	*U primárních aktiv.*		§ 4 odst.2 i)	X	X	
Posoudit dopady na uživatele informačního a komunikačního systému.	*U primárních aktiv.*		§ 4 odst.2 j)	X	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	

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	
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	
Zpracovat zprávu o hodnocení rizik.			§ 5 odst.1 e)	X	X	
Zpracovat na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti.	*Musí obsahovat přehled bezpečnostních opatření požadovaných touto vyhláškou (aplikovnaých i neaplikovaných).*		§ 5 odst.1 f)	X	X	
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 opatření a způsob jejich realizace.*		§ 5 odst.1 g)	X	X	
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	
Zavádět bezpečnostní opatření v souladu s plánem zvládání rizik.			§ 5 odst.1 i)	X	X	
Řízení provozu a komunikací						
Řízení provozu a komunikací						
Stanovit práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role.			§ 10 odst. 1 a)	X	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	X	
Stanovit pravidla a postupy pro sledování KBU a opatření pro ochranu přístupu k záznamům o těchto událostech.			§ 10 odst. 1 c)	X	X	
Stanovit pravidla a postupy pro ochranu před škodlivým kódem.			§ 10 odst. 1 d)	X	X	
Stanovit pravidla a postupy pro řízení technických zranitelností.			§ 10 odst. 1 e)	X	X	
Zajistit spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory.			§ 10 odst. 1 f)	X	X	
Stanovit postupy řízení a schvalování provozních změn.			§ 10 odst. 1 g)	X	X	
Stanovit pravidla a postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.			§ 10 odst. 1 h)	X	X	
Stanovit pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu.			§ 10 odst. 1 i)	X	X	
Stanovit pravidla a postupy pro instalaci technických aktiv.			§ 10 odst. 1 j)	X		
Stanovit provádění pravidelného zálohování a kontroly použitelnosti provedených záloh.			§ 10 odst. 1 k)	X	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	X	
Řídit přístup na základě skupin a rolí.			§ 12 odst. 2 a)	X	X	
Přídělit všem uživatelům a administrátorům přístupová práva a oprávnění a jedinečný identifikátor.			§ 12 odst. 2 b)	X	X	
Řídit identifikátory, přístupová práva, oprávnění aplikací a technických účtů.			§ 12 odst. 2 c)	X	X	
Zavádět bezpečnostní opatření pro řízení přístupu k prostředkům informačního a komunikačního systému.			§ 12 odst. 2 d)	X		
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	X	
Omezit přidělování privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce.			§ 12 odst. 2 f)	X		
Omezit a kontrolovat používání programových prostředků, které mohou být schopné překonat systémové nebo aplikační kontroly.			§ 12 odst. 2 g)	X	X	
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	
Prosazovat, aby uživatelé používali privátních autentizačních informací a dodržovali stanovené postupy.			§ 12 odst. 2 k)	X	X	
Zajistit odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení uživatelů, adiministrátorů nebo osob zastávajících bezpečnostní role.			§ 12 odst. 2 l)	X	X	
Zajistit odebrání nebo změnu přístupových oprávnění při ukončení nebo změně smluvního vztahu.			§ 12 odst. 2 m)	X	X	
Dokumentovat přidělování a odebírání přístupových oprávnění.			§ 12 odst. 2 n)	X	X	
Fyzická bezpečnost						
Předcházet poškození, krádeži nebo zneužití aktiv nebo porušení poskytování služeb informačního a komunikačního systému.			§ 17 odst. a)	X	X	
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		
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		
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		
Využívat autentizační mechanismus.	*Vícefaktorová autentizace.*			X	X	
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	
Monitorovat a řídit používání výměnných zařízení a datových nosičů.			§ 21 odst.1 b)	X	X	
Řídit automatické spouštění obsahu výměnných zařízení a datových nosičů.			§ 21 odst.1 c)	X	X	
Řídit oprávnění ke spuštění kódu.			§ 21 odst.1 d)	X	X	
Provádět pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem.			§ 21 odst.1 e)	X	X	
Kryptografické prostředky						
Používat aktuálně odolné kryptografické algoritmy a kryptografické klíče.			§ 26 odst. a)	X	X	
Používat systém správy klíčů a certifikátů.	*Zajistit generování, distribuci, ukládání změny, omezení platnosti, zněplatnění certifikátů a likvidaci klíčů a umožnit kontrolu a audit.*		§ 26 odst. b)	X	X	
Prosazovat bezpečné nakládání s kryptografickými prostředky.			§ 26 odst. c)	X	X	
Zohledňovat doporučení v oblasti kryptografických prostředků vydaných Úřadem.			§ 26 odst. d)	X	X	
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 bezpešnostní role.*		§ 9 odst. 1 a)	X		
Určit osoby zodpovědné za realizaci jednotlivých činností.			§ 9 odst. 1 b)	X		
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	
Zajistit pravidelná odborná školení pro osoby zastávající bezpečnostní role.			§ 9 odst. 1 d)	X	X	
Zajistit pravidelná školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní.			§ 9 odst. 1 e)	X	X	
Zajistit kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.			§ 9 odst. 1 f)	X	X	

Zajistit předání odpovědnostní v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role.			§ 9 odst. 1 g)	X	X	
Hodnotit účinnost plánu rozvoje bezpečnostního povědomí.			§ 9 odst. 1 h)	X		
Určit pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel.			§ 9 odst. 1 i)	X		
Vést evidence školení a osob, které je absolvovaly.			§ 9 odst. 2	X	X	
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	X	
Řízení kontinuity činností						
Stanovit práva a povinnosti administrátorů a osob zastávajících bezpečnostní role.	*V rámci řízení kontinuity činností.*		§ 15 odst. a)	X	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	
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	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	

Realizovat opatření pro zvýšení odolnosti informačního a komunikačního systému vůči KBI a omezením dostupnosti.			§ 15 odst. f)	X	X	
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	
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	
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	
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	
Zohlednit požadavky vyplývající z bezpečnostních opatření pří 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	Zhotovitel pro své subdodavatele
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	
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				
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				
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				
Hlásit KBI Úřadu.		§ 8 odst.4		X		
Opatření						
Provádět reaktivní opatření.		§ 11 odst.3		X	X	
Oznámit Úřadu reaktivní opatření a jeho výsledek.		§ 13 odst.4		X		
Dokumentace						
1. Bezpečnostní politika				X	X	
1.1. Politika systému řízení bezpečnosti informací				X	X	
1.2. Politika řízení aktiv				X	X	
1.3. Politika organizační bezpečnosti				X	X	
1.4. Politika řízení dodavatelů				X	X	
1.5. Politika bezpečnosti lidských zdrojů				X	X	
1.6 Politika řízení provozu a komunikací				X	X	
1.7. Politika řízení přístupu				X	X	
1.8. Politika bezpečného chování uživatelů				X	X	
1.9. Politika zálohování a obnovy a dlouhodobého ukládání				X	X	
1.10. Politika bezpečného předávání a výměny informací				X	X	
1.11. Politika řízení technických zranitelností				X	X	
1.12. Politika bezpečného používání mobilních zařízení				X	X	
1.13. Politika akvizice, vývoje a údržby				X	X	
1.14. Politika ochrany osobních údajů				X	X	
1.15. Politika fyzické bezpečnosti				X	X	
1.16. Politika bezpečnosti komunikační sítě				X	X	
1.17. Politika ochrany před škodlivým kódem				X	X	
1.18. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí				X	X	
1.19. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí				X	X	

1.20. Politika bezpečného používání kryptografické ochrany				X	X	
1.21. Politika řízení změn				X	X	
1.22. Politika zvládání kybernetických bezpečnostních incidentů				X	X	
1.23. Politika řízení kontinuity činností				X	X	
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	
2.5. Prohlášení o aplikovatelnosti	*Analýza rizik*			X	X	
2.6. Plán zvládání rizik				X	X	
2.7. Plán rozvoje bezpečnostního povědomí				X		
2.8. Evidence změn				X	X	
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		