

## Bezpečnostní opatření pro smluvní vztahy

### 1. ÚVOD

Tato příloha Smlouvy popisuje bezpečnostní požadavky projektu „Informační systém sociálního zabezpečení (DP-3)“ zejména pro naplnění požadavků relevantních k předmětu smlouvy, 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 Prodávajícího a určuje vzájemný vztah odpovědnosti za zavedení a kontrolu bezpečnostních opatření mezi Kupujícím a Prodávajícím. Požadavky na Prodávajícího 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

**Prodávající se při poskytování plnění pro Kupujícího zavazuje plnit následující povinnosti:**

1. postupovat v souladu s účinnými právními předpisy, zejména pak požadavky vyplývajícími pro Prodávajícího, 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) Kupujícího dle specifikace předmětu veřejné zakázky;
2. nejpozději do tří pracovních dnů po dni účinnosti Smlouvy jmenovat za Prodávajícího 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 Prodávajícího“). Kontaktní osobu pro bezpečnost na straně Prodávajícího sdělí písemně Kupujícímu v téže lhůtě;
3. zajistit, aby Kontaktní osoba pro bezpečnost na straně Prodávajícího nejpozději do 30 dnů od uzavření Smlouvy potvrdila písemně Kupujícímu, že všechny osoby podílející se na poskytování plnění této Smlouvy za stranu Prodávajícího a/nebo jeho poddodavatelé byli prokazatelně seznámeni s těmito Bezpečnostními požadavky;
4. poskytovat Kupujícímu součinnost při provádění identifikace a hodnocení aktiv a rizik významného informačního systému v rozsahu aktiv, které jsou součástí dodávaného

řešení a na základě výsledků spolupracovat na návrhu opatření na minimalizaci nebo odstranění zjištěných rizik v rozsahu aktiv, které jsou součástí dodávaného řešení.

5. dodržovat příslušná ustanovení, relevantní k předmětu smlouvy, bezpečnostních politik, metodik a postupů předaných Prodávajícím Kupujícímu, k jejichž dodržování se Prodávající zavázal, pokud byl Prodávající s takovými dokumenty nebo jejich částmi seznámen, a to bez ohledu na způsob, jakým byl s takovou dokumentací Kupujícího seznámen (např. školením, protokolárním předáním příslušné dokumentace Prodávajícímu, elektronickým předáním prostřednictvím e-mailu či datovou schránkou, zřízením přístupu Prodávajícímu na sdílené úložiště aj.); vymezení relevantní části centrální dokumentace ISMS, která byla předána Prodávajícímu, je uvedeno v Příloze č. 6 Smlouvy.
6. zaměstnanci a další osoby na straně Prodávajícího podílející se na plnění Smlouvy musí být prokazatelně seznámeni s platnými předpisy a bezpečnostními požadavky Kupujícího, relevantními s předmětem plnění, a to ještě před zahájením jakékoli činnosti ze strany těchto osob pro Kupujícího v souvislosti s plněním této Smlouvy;
7. zaznamenávat a na vyžádání Kupujícímu poskytnout veškeré podstatné okolnosti související s poskytovaným předmětem plnění dle Smlouvy (technické záznamy, 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 Kupujícího;
9. garantovat dostupnost, důvěrnost plnění a integritu předávaných dat;
10. průběžně dokumentovat, kontrolovat a vyhodnocovat oprávněnost přístupu, jak fyzického, tak i logického, u všech osob na straně Prodávajícího, které přistupují k předmětu plnění dle této Smlouvy;
11. poskytovat Kupujícímu součinnost při zavádění opatření pro ochranu zálohy dat vztahujících se k plnění Smlouvy a pravidelnému testování funkčnosti 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 Kupujícího. Detekované technické zranitelnosti musí být vyhodnoceny s ohledem na související riziko a musí podle povahy předmětu plnění dojít k nápravným opatřením ze strany Prodávajícího. Nápravná opatření musí být schválena Kupujícím;

### **2.3. Oprávnění užívat data**

1. Prodávající je při poskytování plnění pro Kupujícího oprávněn nakládat s daty předanými Prodávajícím Kupujícímu výhradně za účelem plnění předmětu Smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy.
2. Prodávající se při poskytování plnění pro Kupujícího 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. Prodávající je srozuměn s prováděním hodnocení rizik, kontrolou a auditem zavedených bezpečnostních opatření ze strany Kupujícího v souvislosti s poskytovanou službou Prodávající.
2. Hodnocení, kontrola a audit probíhají v intervalech stanovených Kupujícími 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 Prodávajícího nebo jeho poddodavatele a Prodávající má povinnost tyto kontroly a audity Kupujícímu či Kupujícími pověřené osobě umožnit či možnost jejich provedení v prostorách poddodavatele zajistit, přispět k nim a poskytnout Kupujícímu či Kupujícími pověřené osobě k jejich provedení maximální možnou součinnost, kterou lze po Prodávajícímu rozumně požadovat. Počet a frekvence kontrol ani auditů nejsou nijak omezeny.
3. Prodávající je povinen po zavedení opatření provést také vlastní hodnocení rizik a kontrolu zavedených bezpečnostních opatření. Tato kontrola probíhá v pravidelných intervalech stanovených Kupujícími, na žádost Kupujícího 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 Prodávající Kupujícímu bez zbytečného odkladu písemnou kontrolní zprávu.

## 2.5. Řetězení a řízení dodavatelů

**Prodávající se při poskytování plnění pro Kupujícího zavazuje plnit následující povinnosti:**

1. Prodávající nezapojí do poskytování plnění dle této Smlouvy žádného dalšího poddodavatele bez předchozího konkrétního písemného povolení Kupujícího;
2. Prodávající se zavazuje, že se bude řídit požadavky Kupujícího na řízení bezpečnosti informací a poskytne Kupujícímu veškerou nezbytnou součinnost v otázkách řízení bezpečnosti informací a pokud využívá při poskytování plnění poddodavatele, zajistí, že bude Kupujícímu poskytnuta veškerá nezbytná součinnost v otázkách řízení bezpečnosti informací také od těchto poddodavatelů;
3. Prodávající je povinen předat Kupujícímu kontaktní údaje všech osob dodávajících systémovou a technickou podporu pro řešení;
4. Pokud Prodávající využívá při poskytování plnění poddodavatele, zavazuje se, že budou dodržovat bezpečnostní požadavky vč. požadavků na ochranu osobních údajů vyplývající z této Smlouvy. Prodávající se zavazuje bezodkladně doložit Kupujícímu 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, mimo důvěrných informací uvedených ve smluvním vztahu Prodávajícího se svým poddodavatelem, jejichž předložení Kupujícímu by narušilo smluvní vztah Prodávajícího s poddodavatelem;
5. Prodávající 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 Prodávajícího, považuje se každé takové nedodržení požadavků za porušení povinnosti Prodávajícího dle této Smlouvy.

## 2.6. Povinnosti v řízení změn dle ZoKB a VyKB

1. Prodávající se zavazuje v rozsahu předmětu plnění aktivně podílet formou spolupráce na splnění povinností Kupujícího 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. Prodávající se 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. Prodávající se zavazuje aktivně spolupracovat při testování významné změny.

## 2.7. Zvládání bezpečnostních událostí a incidentů

**Prodávající se při poskytování plnění pro Kupujícího zavazuje, že:**

1. bude hlásit všechny bezpečnostní události a incidenty neprodleně po jejich detekci Kupujícímu prostřednictvím ohlašovacích kanálů Kupujícího a v souladu s nastavenými postupy Kupujícího (Politika zvládání KBU a KBI, viz příloha č. 6 Smlouvy), v případech, kdy situace nestrpí odklad, tak 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 Prodávajícího, a rizicích souvisejících s ohrožením kontinuity činností vést záznamy a tyto uchovat pro jejich budoucí použití s ohledem na požadavky Kupujícího a legislativy ČR. Nastavená pravidla a postupy podléhají schválení Kupujícím;
2. nastavená pravidla pro zvládání bezpečnostních incidentů musí respektovat požadavek na legalitu zajištění stop, tj. jejich původ a oprávněnost jejich získání 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. poskytne součinnost Kupujícímu při napojování aktiv, které jsou součástí dodávaného řešení, na monitorovací nástroje Kupujícího a součinnost při zvládání kybernetických bezpečnostních událostí a incidentů Kupujícího a bude se řídit jeho pokyny;
4. provede analýzu příčin bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že Prodávající bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

## 2.8. Informační povinnost a povinnosti při výměně informací

1. Prodávající se během poskytování plnění pro Kupujícího zavazuje Kupujícího 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 Prodávajícího podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných Prodávajícím k plnění na základě smluvního vztahu s Kupujícím.

2. Prodávající se během poskytování plnění pro Kupujícího 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 se ZoKB a VyKB.

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

1. Prodávající se zavazuje poskytnout Kupujícímu součinnost při zpracování plánu řízení KBI a plánu kontinuity a obnovy činností souvisejících s výkonem funkcionality dodávaného řešení.
2. Prodávající se zavazuje dodržovat požadavky Kupujícího na řízení kontinuity činností v souladu se ZoKB, VyKB a ustanoveními bezpečnostních politik, metodik a postupů předaných Prodávajícímu Kupujícím.

### 2.10. Bezpečnost lidských zdrojů

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

### 2.11. Fyzická ochrana a bezpečnost prostředí

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

### 2.12. Požadavky na Řízení přístupu

1. Prodávající bere na vědomí, že přístup k datům, informacím či zařízením souvisejícím s předmětem Smlouvy je možné povolit pouze konkrétním fyzickým osobám / zaměstnancům Prodávajícího / poddodavatele Prodávajícího zaevidovaným, a to na základě požadavku Prodávajícího na přístup.
2. Prodávající bere na vědomí, že přidělení oprávnění zaměstnanci Prodávajícího musí být řízeno zásadou tzv. „potřeba vědět“ (need-to-know principle) a není nárokové.
3. Prodávající se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Prodávajícího nebo poddodavatele Prodávajícího.
4. Prodávající se zavazuje, že nebude instalovat a používat žádné nástroje, které nebyly předem písemně odsouhlaseny Kupujícím přímo nebo nejsou součástí schváleného řešení předmětu Smlouvy.
5. Prodávající 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. Prodávající bere na vědomí, že přístup do interní sítě Kupujícího a/nebo k technologickým a komunikačním systémům Kupujícího bude realizován výhradně s využitím zařízení Kupujícího.

6. Prodávající se zavazuje zajistit, aby osoby podílející se na poskytování plnění Kupujícímu, kteří přistupují do interní sítě a/nebo technologického nebo komunikačního systému chránili autentizační prostředky a údaje k systémům Kupujícího. Prodávající bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako bezpečnostní incident ve smyslu příslušné řídicí dokumentace a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu platí pro Prodávajícího, pokud byl s takovou řídicí dokumentací Kupujícího seznámen).
7. Prodávající bere na vědomí, že postup zvládání bezpečnostního incidentu či skutečnosti vzniklé v důsledku porušení Bezpečnostních požadavků ze strany Prodávajícího nebude posuzována jako okolnost vylučující odpovědnost Prodávajícího za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Prodávajícímu či jiné osobě ze strany Prodávajícího. Ostatní ustanovení ohledně odpovědnosti Prodávajícího za prodlení obsažená v Smlouvě nejsou tímto ustanovením dotčena.

#### **2.13. Monitorování činností**

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

#### **2.14. Předání a převzetí plnění**

1. Prodávající se zavazuje dodržovat Bezpečnostní požadavky i při předání a převzetí plnění dle této Smlouvy
2. Kupující je oprávněn z důvodu nedodržení Bezpečnostních požadavků odmítnout převzetí (části) plnění Smlouvy.

#### **2.15. Likvidace dat**

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

#### **2.16. Sankce**

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

### **2.17. Způsob distribuce dokumentů Kupujícímu**

Prodávající má právo vyžádat si od Kupujícího shora uvedené dokumenty vymezené v Příloze č. 6 Smlouvy, které mu budou předány na základě Dohody o zachování mlčenlivosti o důvěrných informacích (NDA).

| Rozdělení zajištění povinností dle ZoKB a VyKB pro IS                                                          |                                                                                                                                   | DP-3        |                      | Zajišťuje |                    | Poznámka                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------------|----------------------|-----------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Znění povinnosti z ustanovení ZoKB a VyKB                                                                      |                                                                                                                                   | ZoKB        | VyKB                 | Správce   | Významný dodavatel | Poznámka                                                                                                                                            |
|                                                                                                                |                                                                                                                                   | §, odstavec | §, odstavec          | Kupující  | Prodávající        |                                                                                                                                                     |
| Systém řízení bezpečnostní informací                                                                           |                                                                                                                                   |             |                      |           |                    |                                                                                                                                                     |
| ISMS a organizační bezpečnost                                                                                  |                                                                                                                                   |             |                      |           |                    |                                                                                                                                                     |
| Stanovit rozsah ISMS a určit v něm organizační části a aktiva, kterých se ISMS týká.                           |                                                                                                                                   |             | § 3 písm. a)         | X         |                    |                                                                                                                                                     |
| Stanovit cíle ISMS.                                                                                            |                                                                                                                                   |             | § 3 písm. b)         | X         |                    |                                                                                                                                                     |
| Zavést přiměřená bezpečnostní opatření pro ISMS pro stanovený rozsah systému.                                  |                                                                                                                                   |             | § 3 písm. c)         | X         | X                  | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. Podrobnější specifikace bezpečnostních opatření viz níže. |
| Řídit rizika podle § 5 VyKB.                                                                                   |                                                                                                                                   |             | § 3 písm. d)         | X         | X                  | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení.                                                           |
| Vytvořit a schválit bezpečnostní politiku ISMS.                                                                | Musí obsahovat zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti.                             |             | § 3 písm. e)         | X         |                    |                                                                                                                                                     |
| Zajistit provedení auditu KB.                                                                                  |                                                                                                                                   |             | § 3 písm. 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 písm. g)         | X         |                    |                                                                                                                                                     |
| Identifikovat a řídit významné změny.                                                                          | Podle § 11.                                                                                                                       |             | § 3 písm. h)         | X         | X                  | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení.                                                           |
| Aktualizovat ISMS a příslušnou dokumentaci.                                                                    | Na základě výsledků auditu KB, výsledků vyhodnocení účinnosti systému ISMS a v souvislosti s prováděnými významnými změnami.      |             | § 3 písm. i)         | X         | X                  | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení.                                                           |
| Řídit provoz a zdroje ISMS.                                                                                    | Zaznamenávat činnosti spojené s ISMS a řízením rizik.                                                                             |             | § 3 písm. j)         | X         |                    |                                                                                                                                                     |
| Organizační bezpečnost                                                                                         |                                                                                                                                   |             |                      |           |                    |                                                                                                                                                     |
| Zajistit stanovení bezpečnostní politiky a cílů ISMS.                                                          |                                                                                                                                   |             | § 6 odst. 1 písm. a) | X         |                    |                                                                                                                                                     |
| Zajistit integraci ISMS do procesů povinné osoby.                                                              |                                                                                                                                   |             | § 6 odst. 1 písm. b) | X         |                    |                                                                                                                                                     |
| Zajistit dostupnost zdrojů potřebných pro ISMS.                                                                |                                                                                                                                   |             | § 6 odst. 1 písm. c) | X         |                    |                                                                                                                                                     |
| Informovat zaměstnance o významu ISMS a o významu dosažení shody s jeho požadavky se všemi dotčenými stranami. |                                                                                                                                   |             | § 6 odst. 1 písm. d) | X         | X                  | Prodávající informuje v rámci svých zaměstnanců, kteří se podílí na dodávaném řešení.                                                               |
| Zajistit podporu k dosažení zamýšlených výstupů ISMS.                                                          |                                                                                                                                   |             | § 6 odst. 1 písm. e) | X         |                    |                                                                                                                                                     |
| Vést zaměstnance k rozvíjení efektivity ISMS.                                                                  |                                                                                                                                   |             | § 6 odst. 1 písm. f) | X         |                    |                                                                                                                                                     |
| Prosazovat neustálé zlepšování ISMS.                                                                           |                                                                                                                                   |             | § 6 odst. 1 písm. g) | X         |                    |                                                                                                                                                     |
| Podporovat osoby zastávající bezpečnostní role při prosazování KB v oblastech jejich odpovědnosti.             |                                                                                                                                   |             | § 6 odst. 1 písm. h) | X         |                    |                                                                                                                                                     |
| Zajistit stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role.          |                                                                                                                                   |             | § 6 odst. 1 písm. i) | X         |                    |                                                                                                                                                     |
| Zajistit zachování mlčenlivosti administrátorů a osob zastávajících bezpečnostní role.                         |                                                                                                                                   |             | § 6 odst. 1 písm. j) | X         | X                  | Prodávající zajišťuje u svých zaměstnanců v rozsahu dodávaného řešení.                                                                              |
| Zajistit pro osoby, které zastávají bezpečnostní role, příslušné pravomoci a zdroje.                           | Včetně rozpočtových prostředků k naplňování jejich rolí.                                                                          |             | § 6 odst. 1 písm. k) | X         |                    |                                                                                                                                                     |
| Zajistit testování plánu kontinuity činností, obnovy a procesů spojených se zvládáním KBI.                     |                                                                                                                                   |             | § 6 odst. 1 písm. l) | X         | X                  | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení.                                                           |
| Určit složení VKB a bezpečnostní role a jejich práva a povinnosti související s ISMS.                          |                                                                                                                                   |             | § 6 písm. 2          | X         |                    |                                                                                                                                                     |

|                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                     |  |                      |   |   |                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|----------------------|---|---|-----------------------------------------------------------------------------------------------|
| Určit osoby, které budou zastávat bezpečnostní role.                                                                                                                      | <i>MKB, architekt KB, auditor KB, garant aktiva.</i>                                                                                                                                                                                                                                                                                                                |  | § 6 písm. 3          | X |   |                                                                                               |
| <b>Oblast akvizice, vývoje a údržby</b>                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                     |  |                      |   |   |                                                                                               |
| <b>Řízení dodavatelů</b>                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                     |  |                      |   |   |                                                                                               |
| Stanovit pravidla pro dodavatele.                                                                                                                                         | <i>Zohledňovat požadavky ISMS.</i>                                                                                                                                                                                                                                                                                                                                  |  | § 8 odst. 1 písm. a) | X |   |                                                                                               |
| Vést evidenci svých významných dodavatelů.                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                     |  | § 8 odst. 1 písm. b) | X |   |                                                                                               |
| Prokazatelně písemně informovat své významné dodavatele o jejich evidenci.                                                                                                | <i>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).</i> |  | § 8 odst. 1 písm. c) | X |   |                                                                                               |
| Seznamovat své dodavatele se stanovenými pravidly a požadovat dodržení těchto pravidel.                                                                                   | <i>Viz § 8 odst. 1 a)</i>                                                                                                                                                                                                                                                                                                                                           |  | § 8 odst. 1 písm. d) | X | X | Prodávající činnost zajišťuje pro své dodavatele, kteří se budou podílet na dodávaném řešení. |
| Řídit rizika spojené s dodavateli.                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                     |  | § 8 odst. 1 písm. e) | X | X | Prodávající činnost zajišťuje pro své dodavatele, kteří se budou podílet na dodávaném řešení. |
| Zajistit, aby smlouvy uzavírané s významnými dodavateli obsahovaly informace uvedené v příloze č. 7 VyKB.                                                                 | <i>Příloha č. 7 - Řízení dodavatelů – bezpečnostní opatření pro smluvní vztahy.</i>                                                                                                                                                                                                                                                                                 |  | § 8 odst. 1 písm. f) | X |   |                                                                                               |
| Přezkoumávat plnění smluv s významnými dodavateli z hlediska ISMS.                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                     |  | § 8 odst. 1 písm. g) | X |   |                                                                                               |
| V rámci výběrového řízení a před uzavřením smlouvy provést hodnocení rizik souvisejících s předmětem smlouvy.                                                             | <i>U významných dodavatelů.</i>                                                                                                                                                                                                                                                                                                                                     |  | § 8 odst. 2 písm. a) | X |   |                                                                                               |
| V rámci uzavíraných smluv stanovit způsoby a realizace bezpečnostního opatření. Určit obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření. | <i>U významných dodavatelů.</i>                                                                                                                                                                                                                                                                                                                                     |  | § 8 odst. 2 písm. b) | X |   |                                                                                               |
| Provádět pravidelné hodnocení rizik a pravidelnou kontrolu bezpečnostních opatření.                                                                                       | <i>U významných dodavatelů.</i>                                                                                                                                                                                                                                                                                                                                     |  | § 8 odst. 2 písm. c) | X |   |                                                                                               |
| Zajistit řešení rizik a zjištěných nedostatků.                                                                                                                            | <i>U významných dodavatelů.</i>                                                                                                                                                                                                                                                                                                                                     |  | § 8 odst. 2 písm. d) | X |   |                                                                                               |
| <b>Akvize, vývoj a údržba</b>                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                     |  |                      |   |   |                                                                                               |
| Řídit rizika podle § 5 VyKB.                                                                                                                                              | <i>V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému.</i>                                                                                                                                                                                                                                                                 |  | § 13 písm. a)        | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení.    |
| Řídit významné změny podle § 11.                                                                                                                                          | <i>V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému.</i>                                                                                                                                                                                                                                                                 |  | § 13 písm. b)        | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení.    |
| Stanovit bezpečnostní požadavky.                                                                                                                                          | <i>V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému.</i>                                                                                                                                                                                                                                                                 |  | § 13 písm. c)        | X |   |                                                                                               |
| Zahrnout stanovené požadavky do projektu akvizice, vývoje a údržby.                                                                                                       | <i>V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému.</i>                                                                                                                                                                                                                                                                 |  | § 13 písm. d)        | X | X | Prodávající zahrnuje požadavky Kupujícího do svých projektů v rozsahu dodávaného řešení.      |
| Zajistit bezpečnost vývojového a testovacího prostředí a ochranu používaných testovacích dat.                                                                             | <i>V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému.</i>                                                                                                                                                                                                                                                                 |  | § 13 písm. e)        | X |   |                                                                                               |
| Provádět bezpečnostní testování významných změn před jejich uvedením do provozu.                                                                                          | <i>V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému.</i>                                                                                                                                                                                                                                                                 |  | § 13 písm. f)        | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení.    |
| Plnit požadavek podle § 19 odst. 3, je-li cílem provedení akvizice nebo vývoje nástroj pro správu a ověřování identity.                                                   | <i>V souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému.</i>                                                                                                                                                                                                                                                                 |  | § 13 písm. g)        | X | X | Prodávající zahrnuje požadavek do svých projektů v rozsahu dodávaného řešení.                 |
| <b>Řízení změn</b>                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                     |  |                      |   |   |                                                                                               |

|                                                                                                               |                                                                                     |  |                       |   |   |                                                                                            |
|---------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--|-----------------------|---|---|--------------------------------------------------------------------------------------------|
| Přezkoumávat možné dopady změn.                                                                               |                                                                                     |  | § 11 odst. 1 písm. a) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení. |
| Určovat významné změny.                                                                                       |                                                                                     |  | § 11 odst. 1 písm. b) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení. |
| Dokumentovat řízení významných změn.                                                                          |                                                                                     |  | § 11 odst. 2 písm. a) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení. |
| Provádět analýzu rizik.                                                                                       | <i>U významných změn.</i>                                                           |  | § 11 odst. 2 písm. b) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení. |
| Přijímat opatření za účelem snížení všech nepříznivých dopadů významných změn.                                |                                                                                     |  | § 11 odst. 2 písm. c) | X | X | Prodávající přímá opatření na své straně v rozsahu dodávaného řešení.                      |
| Aktualizovat bezpečnostní politiku a dokumentaci.                                                             | <i>U významných změn.</i>                                                           |  | § 11 odst. 2 písm. d) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení. |
| Zajistit testování významných změn.                                                                           |                                                                                     |  | § 11 odst. 2 písm. e) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení. |
| Zajistit možnost navrácení do původního stavu.                                                                | <i>U významných změn.</i>                                                           |  | § 11 odst. 2 písm. f) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení. |
| Rozhodovat o penetračním testování nebo testování zranitelností.                                              | <i>Rozhoduje na základě výsledků analýzy rizik.</i>                                 |  | § 11 odst. 3          | X |   |                                                                                            |
| <b>Řízení aktiv a rizik</b>                                                                                   |                                                                                     |  |                       |   |   |                                                                                            |
| <b>Řízení aktiv</b>                                                                                           |                                                                                     |  |                       |   |   |                                                                                            |
| Stanovit metodiku pro identifikaci aktiv.                                                                     |                                                                                     |  | § 4 odst. 1 písm. a)  | X |   |                                                                                            |
| Stanovit metodiku pro hodnocení aktiv.                                                                        | <i>V rozsahu alespoň dle přílohy č. 1 VyKB.</i>                                     |  | § 4 odst. 1 písm. b)  | X |   |                                                                                            |
| Identifikovat a evidovat aktiva.                                                                              |                                                                                     |  | § 4 odst. 1 písm. c)  | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení. |
| Určit a evidovat garanty aktiv.                                                                               |                                                                                     |  | § 4 odst. 1 písm. d)  | X |   |                                                                                            |
| Hodnotit a evidovat primární aktiva z hlediska důvěrnosti, integrity a dostupnosti.                           | <i>Zařadit tato aktiva dle stanovené metodiky pro hodnocení aktiv.</i>              |  | § 4 odst. 1 písm. e)  | X |   |                                                                                            |
| Určit a evidovat vazby mezi primárními a podpůrnými aktivy.                                                   | <i>Hodnotit důsledky jejich vzájemné závislosti.</i>                                |  | § 4 odst. 1 písm. f)  | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení. |
| Hodnotit podpůrná aktiva.                                                                                     | <i>Zohlednit vzájemné závislosti dle §4 odst. 1 f)</i>                              |  | § 4 odst. 1 písm. g)  | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení. |
| Stanovit a zavádět pravidla ochrany pro jednotlivé úrovně aktiv.                                              | <i>Dle hodnocení aktiv.</i>                                                         |  | § 4 odst. 1 písm. h)  | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení. |
| Stanovit přípustné způsoby používání aktiv a pravidla pro manipulaci s aktivy.                                | <i>Včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv.</i> |  | § 4 odst. 1 písm. i)  | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení. |
| Určit způsob likvidace dat, provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat. | <i>S ohledem na úroveň aktiv a přílohu č. 4 VyKB.</i>                               |  | § 4 odst. 1 písm. j)  | X |   |                                                                                            |
| Posoudit rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství.   | <i>U primárních aktiv.</i>                                                          |  | § 4 odst. 2 písm. a)  | X |   |                                                                                            |
| Posoudit rozsah dotčených právních povinností a jiných závazků.                                               | <i>U primárních aktiv.</i>                                                          |  | § 4 odst. 2 písm. b)  | X |   |                                                                                            |
| Posoudit rozsah narušení vnitřních řídících a kontrolních činností.                                           | <i>U primárních aktiv.</i>                                                          |  | § 4 odst. 2 písm. c)  | X |   |                                                                                            |
| Posoudit poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty.                     | <i>U primárních aktiv.</i>                                                          |  | § 4 odst. 2 písm. d)  | X |   |                                                                                            |
| Posoudit dopady na poskytování důležitých služeb.                                                             | <i>U primárních aktiv.</i>                                                          |  | § 4 odst. 2 písm. e)  | X |   |                                                                                            |
| Posoudit rozsah narušení běžných činností.                                                                    | <i>U primárních aktiv.</i>                                                          |  | § 4 odst. 2 písm. f)  | X |   |                                                                                            |
| Posoudit dopady na zachování dobrého jména nebo ochranu dobré pověsti.                                        | <i>U primárních aktiv.</i>                                                          |  | § 4 odst. 2 písm. g)  | X |   |                                                                                            |
| Posoudit dopady na bezpečnost a zdraví osob.                                                                  | <i>U primárních aktiv.</i>                                                          |  | § 4 odst. 2 písm. h)  | X |   |                                                                                            |
| Posoudit dopady na mezinárodní vztahy.                                                                        | <i>U primárních aktiv.</i>                                                          |  | § 4 odst. 2 písm. i)  | X |   |                                                                                            |
| Posoudit dopady na uživatele informačního a komunikačního systému.                                            | <i>U primárních aktiv.</i>                                                          |  | § 4 odst. 2 písm. j)  | X |   |                                                                                            |
| <b>Řízení rizik</b>                                                                                           |                                                                                     |  |                       |   |   |                                                                                            |

|                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                         |  |                       |   |   |                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-----------------------|---|---|-------------------------------------------------------------------------------------------|
| Stanovit metodiku pro hodnocení rizik.                                                                                                                                      | <i>Včetně stanovení kritérií pro akceptovatelnost rizik.</i>                                                                                                                                                                                                                                                                                            |  | § 5 odst. 1 písm. a)  | X |   |                                                                                           |
| S ohledem na aktiva identifikovat relevantní hrozby a zranitelnosti.                                                                                                        | <i>Zvažovat kategorie hrozeb a zranitelností uvedené v příloze č. 3 VyKB.</i>                                                                                                                                                                                                                                                                           |  | § 5 odst. 1 písm. b)  | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. |
| Provádět hodnocení rizik.                                                                                                                                                   | <i>V pravidelných intervalech (osoba uvedená 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.</i>                                                                                                                                                          |  | § 5 odst. 1 písm. c)  | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. |
| Při hodnocení rizik zohlednit relevantní hrozby a zranitelnosti a posoudit možné dopady na aktiva.                                                                          | <i>Alespoň v rozsahu uvedeném v příloze č.2 VyKB.</i>                                                                                                                                                                                                                                                                                                   |  | § 5 odst. 1 písm. d)  | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. |
| Zpracovat zprávu o hodnocení rizik.                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                         |  | § 5 odst. 1 písm. e)  | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. |
| Zpracovat na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti.                                                                        | <i>Musí obsahovat přehled bezpečnostních opatření požadovaných touto vyhláškou (aplikovaných i neaplikovaných).</i>                                                                                                                                                                                                                                     |  | § 5 odst. 1 písm. f)  | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. |
| Zpracovat a zavést plán zvládání rizik.                                                                                                                                     | <i>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.</i> |  | § 5 odst. 1 písm. g)  | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. |
| Zohledňovat některé atributy při hodnocení rizik v plánu zvládání rizik.                                                                                                    | <i>Atributy: významné změny, změny rozsahu ISMS, opatření podle §11 zákona, KBI včetně již řešených.</i>                                                                                                                                                                                                                                                |  | § 5 odst. 1 písm. h)  | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. |
| Zavádět bezpečnostní opatření v souladu s plánem zvládání rizik.                                                                                                            |                                                                                                                                                                                                                                                                                                                                                         |  | § 5 odst. 1 písm. i)  | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. |
| <b>Řízení provozu a komunikací</b>                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                         |  |                       |   |   |                                                                                           |
| <b>Řízení provozu a komunikací</b>                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                         |  |                       |   |   |                                                                                           |
| Stanovit práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role.                                                                               |                                                                                                                                                                                                                                                                                                                                                         |  | § 10 odst. 1 písm. a) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. |
| 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 písm. b) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. |
| Stanovit pravidla a postupy pro sledování KBU a opatření pro ochranu přístupu k záznamům o těchto událostech.                                                               |                                                                                                                                                                                                                                                                                                                                                         |  | § 10 odst. 1 písm. c) | X |   |                                                                                           |
| Stanovit pravidla a postupy pro ochranu před škodlivým kódem.                                                                                                               |                                                                                                                                                                                                                                                                                                                                                         |  | § 10 odst. 1 písm. d) | X |   |                                                                                           |
| Stanovit pravidla a postupy pro řízení technických zranitelností.                                                                                                           |                                                                                                                                                                                                                                                                                                                                                         |  | § 10 odst. 1 písm. e) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. |
| Zajistit spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory.                                                                             |                                                                                                                                                                                                                                                                                                                                                         |  | § 10 odst. 1 písm. f) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                          |
| Stanovit postupy řízení a schvalování provozních změn.                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                         |  | § 10 odst. 1 písm. g) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. |
| Stanovit pravidla a postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.                                                                       |                                                                                                                                                                                                                                                                                                                                                         |  | § 10 odst. 1 písm. h) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. |
| Stanovit pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu.                                                                                   |                                                                                                                                                                                                                                                                                                                                                         |  | § 10 odst. 1 písm. i) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. |
| Stanovit pravidla a postupy pro instalaci technických aktiv.                                                                                                                |                                                                                                                                                                                                                                                                                                                                                         |  | § 10 odst. 1 písm. j) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. |

|                                                                                                                                                                                                                                |                                                                                                                                              |  |                       |   |   |                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|--|-----------------------|---|---|-------------------------------------------------------------------------------------------|
| Stanovit provádění pravidelného zálohování a kontroly použitelnosti provedených záloh.                                                                                                                                         |                                                                                                                                              |  | § 10 odst. 1 písm. k) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení. |
| Stanovit pravidla a postupy pro zajištění bezpečnosti síťových služeb.                                                                                                                                                         |                                                                                                                                              |  | § 10 odst. 1 písm. l) | X |   |                                                                                           |
| <b>Řízení přístupu</b>                                                                                                                                                                                                         |                                                                                                                                              |  |                       |   |   |                                                                                           |
| 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 písm. 1          | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                          |
| Řídit přístup na základě skupin a rolí.                                                                                                                                                                                        |                                                                                                                                              |  | § 12 odst. 2 písm. a) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                          |
| Přidělit všem uživatelům a administrátorům přístupová práva a oprávnění a jedinečný identifikátor.                                                                                                                             |                                                                                                                                              |  | § 12 odst. 2 písm. b) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                          |
| Řídit identifikátory, přístupová práva, oprávnění aplikací a technických účtů.                                                                                                                                                 |                                                                                                                                              |  | § 12 odst. 2 písm. c) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                          |
| Zavádět bezpečnostní opatření pro řízení přístupu k prostředkům informačního a komunikačního systému.                                                                                                                          |                                                                                                                                              |  | § 12 odst. 2 písm. 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 písm. e) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                          |
| Omezit přidělování privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce.                                                                                                                                  |                                                                                                                                              |  | § 12 odst. 2 písm. f) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                          |
| Omezit a kontrolovat používání programových prostředků, které mohou být schopné překonat systémové nebo aplikační kontroly.                                                                                                    |                                                                                                                                              |  | § 12 odst. 2 písm. g) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                          |
| Přidělovat a odebírat přístupová oprávnění v souladu s politikou řízení přístupu.                                                                                                                                              |                                                                                                                                              |  | § 12 odst. 2 písm. h) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                          |
| Provádět pravidelné přezkoumání nastavení veškerých přístupových oprávnění včetně rozdělení do přístupových skupin a rolí.                                                                                                     |                                                                                                                                              |  | § 12 odst. 2 písm. i) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                          |
| Využívat nástroj pro správu a ověřování identity a nástroj pro řízení oprávnění.                                                                                                                                               |                                                                                                                                              |  | § 12 odst. 2 písm. j) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                          |
| Prosazovat, aby uživatelé používali privátních autentizačních informací a dodržovali stanovené postupy.                                                                                                                        |                                                                                                                                              |  | § 12 odst. 2 písm. k) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                          |
| Zajistit odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.                                                                        |                                                                                                                                              |  | § 12 odst. 2 písm. l) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                          |
| Zajistit odebrání nebo změnu přístupových oprávnění při ukončení nebo změně smluvního vztahu.                                                                                                                                  |                                                                                                                                              |  | § 12 odst. 2 písm. m) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                          |
| Dokumentovat přidělování a odebírání přístupových oprávnění.                                                                                                                                                                   |                                                                                                                                              |  | § 12 odst. 2 písm. n) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                          |
| <b>Fyzická bezpečnost</b>                                                                                                                                                                                                      |                                                                                                                                              |  |                       |   |   |                                                                                           |
| Předcházet poškození, krádeži nebo zneužití aktiv nebo porušení poskytování služeb informačního a komunikačního systému.                                                                                                       |                                                                                                                                              |  | § 17 písm. a)         | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                          |
| Stanovit fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány a zpracovávány informace a umístěna technická aktiva informačního a komunikačního systému.                                                |                                                                                                                                              |  | § 17 písm. 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 písm. c)         | X |   |                                                                                           |
| <b>Bezpečnost komunikační sítě</b>                                                                                                                                                                                             |                                                                                                                                              |  |                       |   |   |                                                                                           |
| Zajistit segmentaci komunikační sítě.                                                                                                                                                                                          |                                                                                                                                              |  | § 18 písm. a)         | X |   |                                                                                           |
| Zajistit řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě.                                                                                                                                              |                                                                                                                                              |  | § 18 písm. b)         | X |   |                                                                                           |

|                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                      |  |                       |   |   |                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-----------------------|---|---|----------------------------------------------------------------------------------------|
| Zajistit pomocí kryptografie důvěrnost a integritu dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do komunikační sítě pomocí bezdrátových technologií.                                                                     |                                                                                                                                                                                                                                                                                                                      |  | § 18 písm. c)         | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                       |
| Aktivně blokovat nežádoucí komunikaci.                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                      |  | § 18 písm. d)         | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                       |
| Pro zajištění segmentace sítě a pro řízení komunikace mezi jejími segmenty využívat nástroj, který zajistí ochranu integrity sítě.                                                                                                        |                                                                                                                                                                                                                                                                                                                      |  | § 18 písm. e)         | X |   |                                                                                        |
| <b>Správa o ověřování identit</b>                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                      |  |                       |   |   |                                                                                        |
| Používat nástroj pro správu a ověření identit uživatelů, administrátorů a aplikací komunikačního a informačního systému.                                                                                                                  |                                                                                                                                                                                                                                                                                                                      |  | § 19 odst. 1          | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                       |
| Využívat autentizační mechanismus.                                                                                                                                                                                                        | Vícefaktorová autentizace.                                                                                                                                                                                                                                                                                           |  |                       | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                       |
| <b>Ochrana před škodlivým kódem</b>                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                      |  |                       |   |   |                                                                                        |
| 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 písm. a) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                       |
| Monitorovat a řídit používání výměnných zařízení a datových nosičů.                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                      |  | § 21 odst. 1 písm. b) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                       |
| Řídit automatické spouštění obsahu výměnných zařízení a datových nosičů.                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                      |  | § 21 odst. 1 písm. c) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                       |
| Řídit oprávnění ke spuštění kódu.                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                      |  | § 21 odst. 1 písm. d) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                       |
| Provádět pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem.                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                      |  | § 21 odst. 1 písm. e) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                       |
| <b>Kryptografické prostředky</b>                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                      |  |                       |   |   |                                                                                        |
| Používat aktuálně odolné kryptografické algoritmy a kryptografické klíče.                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                      |  | § 26 odst. písm. a)   | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                       |
| 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. písm. b)   | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                       |
| Prosazovat bezpečné nakládání s kryptografickými prostředky.                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                      |  | § 26 odst. písm. c)   | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                       |
| Zohledňovat doporučení v oblasti kryptografických prostředků vydaných Úřadem.                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                      |  | § 26 odst. písm. d)   | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                       |
| <b>Bezpečnost lidských zdrojů</b>                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                      |  |                       |   |   |                                                                                        |
| 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 písm. a)  | X |   |                                                                                        |
| Určit osoby zodpovědné za realizaci jednotlivých činností.                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                      |  | § 9 odst. 1 písm. 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 písm. c)  | X | X | Prodávající zajišťuje na své straně pro zaměstnance podílející se na dodávaném řešení. |
| Zajistit pravidelná odborná školení pro osoby zastávající bezpečnostní role.                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                      |  | § 9 odst. 1 písm. d)  | X |   |                                                                                        |
| Zajistit pravidelná školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní.                                                                                                                           |                                                                                                                                                                                                                                                                                                                      |  | § 9 odst. 1 písm. e)  | X | X | Prodávající zajišťuje na své straně pro zaměstnance podílející se na dodávaném řešení. |

|                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                         |  |                       |   |   |                                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-----------------------|---|---|--------------------------------------------------------------------------------------------|
| Zajistit kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.                          |                                                                                                                                                                                                                                                                                                                                                                                         |  | § 9 odst. 1 písm. f)  | X | X | Prodávající zajišťuje na své straně pro zaměstnance podílející se na dodávaném řešení.     |
| Zajistit předání odpovědnosti v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role.                           |                                                                                                                                                                                                                                                                                                                                                                                         |  | § 9 odst. 1 písm. g)  | X | X | Prodávající zajišťuje na své straně pro zaměstnance podílející se na dodávaném řešení.     |
| Hodnotit účinnost plánu rozvoje bezpečnostního povědomí.                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                         |  | § 9 odst. 1 písm. h)  | X |   |                                                                                            |
| Určit pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel.                                                               |                                                                                                                                                                                                                                                                                                                                                                                         |  | § 9 odst. 1 písm. i)  | X |   |                                                                                            |
| Vést evidence školení a osob, které je absolvovaly.                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                         |  | § 9 odst. 2           | X | X | Prodávající zajišťuje na své straně pro zaměstnance podílející se na dodávaném řešení.     |
| <b>Řízení kontinuity činností</b>                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                         |  |                       |   |   |                                                                                            |
| <b>Detekce kybernetických bezpečnostních událostí</b>                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                         |  |                       |   |   |                                                                                            |
| Ověřit a kontrolovat přenášená data v rámci komunikační sítě a mezi komunikačními sítěmi.                                                               |                                                                                                                                                                                                                                                                                                                                                                                         |  | § 23 odst. 1 písm. a) | X |   |                                                                                            |
| Ověřit a kontrolovat přenášená data na perimetru komunikační sítě.                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                         |  | § 23 odst. 1 písm. b) | X |   |                                                                                            |
| Blokovat nežádoucí komunikaci.                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                         |  | § 23 odst. 1 písm. c) | X |   |                                                                                            |
| Zajistit detekci KBU s ohledem na důležitost aktiv v rámci jednotlivých míst.                                                                           | <i>Koncové stanice, mobilní zařízení, servery, datová úložiště a výměnné datové nosiče, síťové aktivní prvky a obdobná aktiva.</i>                                                                                                                                                                                                                                                      |  | § 23 písm. 2          | X |   |                                                                                            |
| <b>Sběr a vyhodnocení kybernetických bezpečnostní událostí</b>                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                         |  |                       |   |   |                                                                                            |
| Sbírat a vyhodnocovat události zaznamenané dle § 22 a § 23 VyKB.                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                         |  | § 24 písm. a)         | X |   |                                                                                            |
| Vyhledávat a seskupovat související záznamy.                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                         |  | § 24 písm. b)         | X |   |                                                                                            |
| Poskytovat informace pro určené bezpečnostní role o detekovaných KBU.                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                         |  | § 24 písm. c)         | X |   |                                                                                            |
| Vyhodnocovat KBU s cílem identifikace KBU.                                                                                                              | <i>Včetně včasného varování určených bezpečnostních rolí.</i>                                                                                                                                                                                                                                                                                                                           |  | § 24 písm. d)         | X |   |                                                                                            |
| Omezit případy nesprávného vyhodnocení událostí pravidelnou aktualizací pravidel.                                                                       | <i>Pravidla pro vyhodnocování KBU a pro včasné varování.</i>                                                                                                                                                                                                                                                                                                                            |  | § 24 písm. e)         | X |   |                                                                                            |
| Využívat informace získané nástrojem pro sběr a vyhodnocení KBU pro optimální nastavení bezpečnostních opatření informačního a komunikačního systému.   |                                                                                                                                                                                                                                                                                                                                                                                         |  | § 24 písm. f)         | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení. |
| <b>Řízení kontinuity činností</b>                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                         |  |                       |   |   |                                                                                            |
| Stanovit práva a povinnosti administrátorů a osob zastávajících bezpečnostní role.                                                                      | <i>V rámci řízení kontinuity činností.</i>                                                                                                                                                                                                                                                                                                                                              |  | § 15 písm. a)         | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení. |
| Pomocí hodnocení rizik a analýzy dopadů vyhodnotit a dokumentovat možné dopady KBI a posoudit možná rizika související s ohrožením kontinuity činností. |                                                                                                                                                                                                                                                                                                                                                                                         |  | § 15 písm. b)         | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení. |
| Na základě výstupů hodnotit rizika a analýzy dopadů a stanovit cíle řízení kontinuity činností.                                                         | <i>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.</i> |  | § 15 písm. c)         | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícími v rozsahu dodávaného řešení. |
| Stanovit politiku řízení kontinuity činností.                                                                                                           | <i>Musí obsahovat naplnění cílů.</i>                                                                                                                                                                                                                                                                                                                                                    |  | § 15 písm. d)         | X |   |                                                                                            |

|                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                        |             |                       |   |   |                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|-------------|-----------------------|---|---|-------------------------------------------------------------------------------------------------------------------|
| Vypracovat, aktualizovat a pravidelně testovat plány kontinuity činností a havarijní plány související s provozováním informačního a komunikačního systému.                                                                                                                                                                          |                                                                                                                                        |             | § 15 písm. e)         | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení.                         |
| Realizovat opatření pro zvýšení odolnosti informačního a komunikačního systému vůči KBI a omezením dostupnosti.                                                                                                                                                                                                                      |                                                                                                                                        |             | § 15 písm. f)         | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení.                         |
| <b>Zvládání kybernetických bezpečnostních událostí a incidentů</b>                                                                                                                                                                                                                                                                   |                                                                                                                                        |             |                       |   |   |                                                                                                                   |
| Zavést proces detekce a vyhodnocování KBU a zvládání KBI                                                                                                                                                                                                                                                                             |                                                                                                                                        |             | § 14 odst. 1 písm. a) | X |   |                                                                                                                   |
| Přidělení odpovědnosti a stanovení postupů.                                                                                                                                                                                                                                                                                          | <i>Postupy a odpovědnosti pro detekci a vyhodnocování KBI a KBI, pro koordinaci a zvládání KBI.</i>                                    |             | § 14 odst. 1 písm. b) | X |   |                                                                                                                   |
| Definovat a aplikovat postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu KBI.                                                                                                                                                                                                            |                                                                                                                                        |             | § 14 odst. 1 písm. c) | X |   |                                                                                                                   |
| Zajistit detekci KBU.                                                                                                                                                                                                                                                                                                                |                                                                                                                                        |             | § 14 odst. 1 písm. d) | X | X | Prodávající hlásí všechny jím zjištěné bezpečnostní události a incidenty neprodleně po jejich detekci Kupujícímu. |
| Zajistit, že uživatelé, administrátoři, osoby zastávající bezpečnostní role, další zaměstnanci a dodavatelé budou oznamovat neobvyklé chování informačního a komunikačního systému.                                                                                                                                                  |                                                                                                                                        |             | § 14 odst. 1 písm. f) | X | X | Prodávající zajišťuje na své straně pro zaměstnance podílející se na dodávaném řešení.                            |
| Zajistit posuzování KBU.                                                                                                                                                                                                                                                                                                             | <i>Rozhodovat o jejich klasifikaci.</i>                                                                                                |             | § 14 odst. 1 písm. g) | X |   |                                                                                                                   |
| Zajistit zvládání KBI.                                                                                                                                                                                                                                                                                                               |                                                                                                                                        |             | § 14 odst. 1 písm. h) | X |   |                                                                                                                   |
| Přijímat opatření pro odvrácení a zmírnění dopadu KBI.                                                                                                                                                                                                                                                                               |                                                                                                                                        |             | § 14 odst. 1 písm. i) | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                                                  |
| Hlásit KBI NÚKIB.                                                                                                                                                                                                                                                                                                                    |                                                                                                                                        |             | § 14 odst. 1 písm. j) | X |   |                                                                                                                   |
| Vést záznamy o KBI a jejich zvládání.                                                                                                                                                                                                                                                                                                |                                                                                                                                        |             | § 14 odst. 1 písm. k) | X |   |                                                                                                                   |
| Prošetřit a určit příčiny KBI.                                                                                                                                                                                                                                                                                                       |                                                                                                                                        |             | § 14 odst. 1 písm. l) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení.                         |
| Vyhodnotit účinnost řešení KBI.                                                                                                                                                                                                                                                                                                      | <i>Stanovit nutná bezpečnostní opatření nebo aktualizovat stávající.</i>                                                               |             | § 14 odst. 1 písm. m) | X | X | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení.                         |
| <b>Audit kybernetické bezpečnosti</b>                                                                                                                                                                                                                                                                                                |                                                                                                                                        |             |                       |   |   |                                                                                                                   |
| Provádět a dokumentovat dodržování bezpečnostní politiky.                                                                                                                                                                                                                                                                            | <i>Včetně přezkoumání technické shody. Výsledky auditu zohlednit v plánu zvládání rizik a v plánu rozvoje bezpečnostního povědomí.</i> |             | § 16 odst. 1 písm. 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.                                                                                                                                        | <i>Určit případná nápravná opatření.</i>                                                                                               |             | § 16 odst. 1 písm. b) | X |   |                                                                                                                   |
| <b>Bezpečnostní opatření</b>                                                                                                                                                                                                                                                                                                         |                                                                                                                                        |             |                       |   |   |                                                                                                                   |
| 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 | Prodávající se na činnosti podílí a spolupracuje s Kupujícím v rozsahu dodávaného řešení.                         |
| Zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro informační a komunikační systém a tyto požadavky zahrnout do uzavírané smlouvy.                                                                                                                                                                  | <i>Definovat a uplatňovat požadavky do smluv s dodavateli / subdodavateli</i>                                                          | § 4 odst. 4 |                       | X | X | Prodávající činnost zajišťuje pro své dodavatele, kteří se budou podílet na dodávaném řešení.                     |

|                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                         |              |  |   |   |                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|--|---|---|-------------------------------------------------------------------------------------------------------------------------|
| Zajistit si ve smlouvě s dodavatelem cloud computingu dodržování bezpečnostních pravidel pro poskytování služeb cloud computingu stanovených Úřadem.                                                                                                                                                                                                                                      | <i>Musí mít k dispozici na základě své žádosti bez zbytečného odkladu informace a data, která pro ně poskytovatel služeb cloud computingu uchovává.</i> | § 4 odst. 5  |  | X | X | Prodávající činnost zajišťuje pro případné své dodavatele cloud computingu, kteří se budou podílet na dodávaném řešení. |
| 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 infrastruktury 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.                                                                                                                                                                     | <i>Bezodkladně po detekci.</i>                                                                                                                          | § 8 odst. 1  |  | X |   |                                                                                                                         |
| Hlásit KBI provozovateli národního CERT.                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                         | § 8 odst. 3  |  |   |   |                                                                                                                         |
| Hlásit KBI Úřadu.                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                         | § 8 odst. 4  |  | X |   |                                                                                                                         |
| <b>Opatření</b>                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                         |              |  |   |   |                                                                                                                         |
| Provádět reaktivní opatření.                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                         | § 11 odst. 3 |  | X | X | Prodávající zajišťuje na své straně v rozsahu dodávaného řešení.                                                        |
| Oznámit Úřadu reaktivní opatření a jeho výsledek.                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                         | § 13 odst. 4 |  | X |   |                                                                                                                         |

