**Bezpečnostní požadavky na dodavatele a poskytovatele služeb pro smlouvy na údržbu**

# Úvodní ustanovení

Pro potřeby této přílohy Smlouvy jsou použity následující zkratky a pojmy:

|  |  |
| --- | --- |
| **ZoKB** | Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů |
| **Vyhláška nebo VoKB** | Vyhláška 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) |
| **Nařízení** | Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) |
| **Osobní údaje** | Veškeré informace o identifikované nebo identifikovatelné fyzické osobě (například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby). |
| **Zpracování osobních údajů** | Jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení. |
| **Datum podpisu smlouvy** | Datum podpisu této smlouvy nebo datum začlenění těchto Bezpečnostních požadavků do smlouvy prostřednictvím dodatku k této smlouvě |
| **Osoba na straně Poskytovatele** | Fyzická osoba podílející se na poskytování předmětu plnění a mající pracovněprávní či obdobný smluvní vztah s Poskytovatelem nebo jeho poddodavateli |
| **Klasifikační schéma** | Klasifikační schéma určující nakládání s daty a informacemi společnosti Skupiny ÚJV v papírové a elektronické podobě |
| **Prostředí Objednatele** | Fyzický perimetr určený ohraničením fyzického prostoru v nájmu nebo majetku Objednatele anebo logický perimetr definovaný hraničními síťovými prvky ve správě nebo majetku Objednatele |

# Účel

Účelem této přílohy je definovat závazné bezpečnostně provozní požadavky a jejich úroveň pro poskytovatele, jejichž předmětem plnění pro objednatele je údržba a servisní podpora systémů, HW prvků nebo servis software (dále také jen „SW“). Dále je účelem této přílohy definovat závazné bezpečnostně provozní požadavky i pro poskytovatele, kteří v souvislosti s plněním dle smlouvy pro objednatele přistupují ke službám a v této souvislosti k informačním a řídícím komunikačním systémům, a/nebo kteří v rámci poskytovaného plnění pro objednatele zpracovávají, a/nebo přenášejí a/nebo ukládají a/nebo archivují jakákoli data a informace objednatele (dále také jen „Bezpečnostně provozní požadavky“).

1. Dále je účelem tohoto dokumentu definovat požadavky na dodavatele dle ISO/IEC 27001 a platné právní úpravy, především pak dle ustanovení § 5 odst. 2 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění, a § 8 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), v platném znění, přičemž zohledňuje také ostatní související platné právní předpisy týkající se dané problematiky.
2. Bezpečnostně provozní požadavky se poskytovatel zavazuje v souladu s platnou právní úpravou, zejména pak výše uvedenými právními předpisy zavést, přičemž za jejich zavedení odpovídá v plném rozsahu objednateli.

# Bezpečnostně provozní požadavky a opatření

### 2.1 Systém řízení bezpečnosti informací

1. Poskytovatel bere na vědomí, že Objednatel má zaveden systém řízení bezpečnosti informací dle ISO/IEC 27001 a zároveň je osobou dle § 3 odst. c) a d), příp. f) a g) ZoKB a je povinen naplnit požadavky související legislativy.
2. Požadavky informační bezpečnosti jsou součástí závazných podmínek spolupráce s externím subjektem, se závazností pro třetí strany. Pověřený zaměstnanec společnosti náležející do Skupiny ÚJV (Osoba oprávněná jednat za objednatele ve věcech technických a realizačních, ve vztahu k organizační struktuře objednatele Vedoucí pracovníci jako vlastníci informačních aktiv a Manažer informační a kybernetické bezpečnosti, Manažer ochrany), oprávněný k jednání v oblasti informační bezpečnosti musí zajistit požadavky informační bezpečnosti Skupiny ÚJV ve vztahu k externímu subjektu (dodavateli) a se závazností pro třetí strany, v souladu s požadavky vlastníka informačních aktiv.
3. Poskytovatel se při poskytování plnění pro Objednatele zavazuje plnit následující povinnosti:
4. pokud poskytovatel využívá při poskytování plnění poddodavatele, poskytovatel se zavazuje zajistit dodržování Bezpečnostně provozních požadavků rovněž ve smluvních vztazích se svými poddodavateli;
5. jmenovat nejpozději do 5 dnů od prokazatelného převzetí těchto Bezpečnostně provozních požadavků zodpovědnou kontaktní osobu pro potřeby zajištění plnění těchto Bezpečnostně provozních požadavků a související komunikaci mezi smluvními stranami (dále také jen „Kontaktní osoba pro bezpečnost na straně poskytovatele[[1]](#footnote-2)“). Kontaktní osobu pro bezpečnost na straně poskytovatele sdělí písemně objednateli v téže lhůtě. Objednatel stanovuje, že určení Kontaktní osoby pro bezpečnost na straně poskytovatele nemá dopad na ustanovení týkající se Oprávněných osob smluvních stran, je-li/jsou-li toto/tato ustanovení ve smlouvě na údržbu použita;
6. zajistit, aby Kontaktní osoba pro bezpečnost na straně poskytovatele bezodkladně po svém jmenování určila rozsah a popsala dotčená aktiva potřebná pro plnění těchto Bezpečnostně provozních požadavků na systémech ICT objednatele (aktivy se rozumí např. data a informace, systémy ICT, moduly, HW prvky, aplikace, databáze, servery, úložiště, koncová zařízení – pracovní stanice typu osobní počítač nebo notebook apod. užívaná pro údržbu systémů ICT objednatele);
7. pokud při plnění těchto Bezpečnostně provozních požadavků nebo při plnění uzavřené smlouvy dochází ke zpracování osobních údajů, Kontaktní osoba pro bezpečnost na straně poskytovatele se zavazuje informovat ve smyslu nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „Nařízení“) své poddodavatele o zpracování jejich osobních údajů a osobních údajů jejich zaměstnanců, případně zajistit uzavření samostatných smluv o zpracování osobních údajů ve smyslu příslušných ustanovení Nařízení
8. dodržovat veškerá ustanovení Nařízení. Poskytovatel je povinen přijmout veškerá opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití;
9. poskytovatel se zavazuje, že nebude poskytovat data ze systémů ICT třetí straně.
10. poskytovat pravidelné reporty - tj. vytvářet a poskytovat zprávy o hodnocení aktiv a provádět identifikaci rizik a sestavit plán jejich zvládání ve vztahu k poskytovanému plnění. Zprávu o hodnocení aktiv i plán zvládání rizik se poskytovatel zavazuje předkládat na vyžádání objednateli 1x ročně vždy ke konci měsíce ledna za předcházející kalendářní rok. Zpráva o hodnocení aktiv bude vždy sestávat z následujících kapitol:
11. Manažerské shrnutí
12. Zpráva o stavu kybernetické bezpečnosti za hodnocený rok
13. Realizovaná bezpečnostní opatření
14. Vyhodnocení bezpečnostních událostí a incidentů
15. Nepokrytá bezpečnostní rizika a návrh opatření
16. Stav souladu s bezpečnostní legislativou
17. Závěr, doporučení

Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na dodržování Bezpečnostně provozních požadavků, provozu a rozvoji bezpečnostních opatření Objednatele a zároveň se zavazuje:

1. Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Poskytovatele při poskytování předmětu plnění.
2. Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění.
3. Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost.
4. Vytvořit a schválit bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Poskytovatele při poskytování předmětu plnění. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.
5. Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.
6. Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy Objednateli zpřístupnit.
7. Po skončení plnění smlouvy bez zbytečného odkladu skartovat veškeré informace a data Objednatele, které mu byly v souvislosti s plněním smlouvy předány.

### 2.2 Bezpečnost lidských zdrojů

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na dodržování, provozu a rozvoji bezpečnostních opatření Objednatele a zároveň se zavazuje plnit následující povinnosti:
2. Zajistit, aby Odpovědná osoba ve věcech smluvních nejpozději do 10 dnů od uzavření smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování předmětu plnění za stranu Poskytovatele byly prokazatelně seznámeny s těmito Bezpečnostními požadavky a s pravidly CYBEX (Pravidla kybernetické bezpečnosti pro externí pracovníky).
3. Využívat pro poskytování předmětu plnění pouze oprávněných osob, které byly řádně seznámeny s pravidly CYBEX a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění. Realizovat rozvoj bezpečnostního povědomí svých zaměstnanců, kteří se podílejí na plnění realizovaném pro poskytovatele na systémech ICT objednatele, a to nejméně jednou za tři roky nebo vždy v souvislosti s prováděnými nebo plánovanými změnami. Zaměstnanci poskytovatele musí být prokazatelně seznámeni s platnými právními předpisy a Bezpečnostně provozními požadavky objednatele
4. Dodržovat příslušná ustanovení interních řídicích aktů Skupiny ÚJV a Skupiny ČEZ v rozsahu, v jakém byl s těmito akty prokazatelně seznámen. Za prokazatelné seznámení se považuje školení pracovníků Poskytovatele zajištěné Objednatelem, protokolární či elektronické předání příslušné dokumentace nebo Objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní řídící akty.
5. V případě, že je součástí předmětu plnění služba dohledu nad předmětem plnění, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu plnění.
6. Zajistit, aby osoby podílející se na poskytování plnění Objednateli v prostředí nebo s prostředky Objednatele, a to i tehdy, pokud jsou prostředky Objednatele používány mimo jeho prostředí:
   1. Pro uložení a sdíleni dat a informací Objednatele využívaly pouze k tomu schválené prostředky;
   2. Neukládaly ani nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;
   3. Nestahovaly, nesdílely, neukládaly, nearchivovaly ani neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem;
   4. Nenavštěvovaly internetové stránky s eticky nevhodným obsahem; [[2]](#footnote-3)
   5. Nerealizovaly pokusy o neautorizovaný přístup ke zdrojům Objednatele ani ke zdrojům jiných subjektů;
   6. Nerealizovaly pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků Objednatele, a to ani v případě, kdy jim byl prostředek Objednatele svěřen do správy;
   7. Nepodílely se s prostředky Objednatele na šíření spamu ani škodlivého softwaru.
   8. Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění objednateli na systémech ICT objednatele, vykonávaly pouze činnosti v souladu s projektovou a provozní dokumentací.
7. Poskytovatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům Objednatele je na straně Objednatele zpracování osobních údajů pracovníků Poskytovatele, kteří se podílejí na zajištění předmětu plnění. Pokud nebude Objednateli umožněno osobní údaje dotčených pracovníků Poskytovatele zpracovat, nebude těmto pracovníkům umožněn žádný přístup ke zdrojům Objednatele.

### 2.3 Řízení provozu a komunikací

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na dodržování, provozu a rozvoji bezpečnostních opatření Objednatele a zároveň se zavazuje:
2. Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění.
3. Na vyžádání poskytnout Objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.
4. Zajistit, že pro poskytování předmětu plnění budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou a evropskou legislativou, především s ohledem na licenční podmínky a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, v platném znění.

### 2.4 Řízení přístupu a bezpečné chování uživatelů

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na dodržování, provozu a rozvoji bezpečnostních opatření Objednatele a zároveň se zavazuje:
2. Přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele.
3. Zajistit, aby udělený přístup nebyl sdílen více osobami za stranu Poskytovatele.
4. Stanovit v požadavku na přístup rozsah dat/informací, služby, účelu, pro které je přístup k systému ICT objednatele požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou / 1 rok / 1 měsíc / 1 den).
5. Zajistit, aby osoby podílející se na poskytování předmětu plnění a mající přístup k informačním aktivum Skupiny ÚJV nebo Skupiny ČEZ chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.
6. Průběžně kontrolovat a vyhodnocovat oprávněnost přístupu, jak fyzického, tak i logického, u všech osob na straně Poskytovatele, které přistupují do prostředí Objednatele.
7. Poskytovatel bere na vědomí, že přístup k systému ICT společností Skupiny ÚJV je možné povolit pouze fyzické identitě zaměstnance poskytovatele / poddodavatele poskytovatele ověřené dokladem totožnosti a pro přístup do ICT systému s vygenerovaným jednoznačným identifikátorem, dále pak zaevidované v registru identit, a to na základě požadavku Poskytovatele na přístup. Pro zaevidování v registru identit, a to na základě požadavku poskytovatele. Pro zaregistrování v registru identit je nezbytné sdělení těchto osobních údajů zaměstnance Poskytovatele:
   * 1. Jméno (Registr identit)
     2. Příjmení (Registr identit)
     3. Rodné příjmení (Registr identit)
     4. Pohlaví (pouze při ověření, bez záznamu v registru identit)
     5. Datum narození (Registr identit)
     6. Rodné číslo (pouze při ověření, bez záznamu v registru identit, RČ v systémech neukládáme, nepožadujeme jeho zasílání ani zaznamenání do formuláře ale je vyžadováno při ověření fyzické identity, kdy toto fyzická identita sdělí v okamžiku ověření. V případě nesouhlasu fyzické osoby s použitím RČ je ověření provedeno na základě data narození a dalších osobních údajů fyzické osoby).
     7. Email (Registr identit)
     8. Mobilní telefon případně pevná linka (Registr identit)
8. Poskytovatel se zavazuje informovat ve smyslu Nařízení své zaměstnance a poddodavatele, kterým bude přidělen přístup (fyzický, logický) k systému ICT, o způsobu zpracování jejich osobních údajů a objednatel se zavazuje zpracovávat osobní údaje výhradně v souladu s Nařízením.
9. Poskytovatel bere na vědomí, že činnost uživatelů přistupujících k informačním systémům objednatele pomocí privilegovaných uživatelských účtů může být monitorována a zaznamenávána pro účely bezpečnostního auditu, vyšetřování bezpečnostních incidentů a zajištění souladu s interními bezpečnostními politikami objednatele.
10. Uživatel je o aktivním zaznamenávání své činnosti vždy jednoznačně informován při zahájení relace.
11. Poskytovatel se zavazuje informovat všechny dotčené osoby (např. zaměstnance, subdodavatele, partnery), které se budou podílet na plnění této smlouvy a přistupovat k výše uvedeným systémům, o možnosti tohoto monitorování a zaznamenávání.
12. Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci poskytovatele musí být řízeno principem nezbytného minima a není nárokové.
13. Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele (osoby za stranu Poskytovatele) může být příslušný účet zablokován a řešen jako bezpečnostní incident a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům).

### 2.5 Akvizice, vývoj a údržba

Požadavky na systémovou a provozní bezpečnostní dokumentaci Systémů ICT objednatele

Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na dodržování, provozu a rozvoji bezpečnostních opatření Objednatele a zároveň se zavazuje:

1. Zajistit bezpečnou implementaci, inovaci, aktualizaci, údržbu a testování technologií a zálohování a archivaci dat, pokud jsou předmětem plnění.
2. Předat Objednateli dokumentaci předmětu plnění minimálně v následujícím rozsahu:
3. dokumentaci skutečného provedení,
4. dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů,
5. dokumentaci obsahující popis autorizačního konceptu a oprávnění,
6. dokumentaci obsahující zálohovací a archivační postupy,
7. dokumentaci obsahující instalační a konfigurační postupy,
8. dokumentaci pro zajištění kontinuity provozu tj. strategie obnovy po havárii (pro systémy klasifikované z pohledu dostupnosti jako „A“).
9. Poskytovatel se zavazuje, že pro všechny ICT systémy poskytovatele (včetně paměťových médií), které se připojují do prostředí objednatele, je a bude zajištěna účinná ochrana proti malware,
10. dodržovat postupy pro zálohování dat a programového vybavení (SW) dané projektovou a provozní dokumentací. Všechny zálohy prováděné poskytovatelem, vč. zálohovacích médií musí být chráněny;
11. průběžně detekovat technické zranitelnosti a konfigurační nesoulady předmětu plnění v procesu výkonu údržby na systémech ICT objednatele. Detekované technické zranitelnosti musí být vyhodnoceny s ohledem na související riziko a musí podle povahy předmětu plnění dojít k nápravným opatřením ze strany poskytovatele;
12. zajistit, aby instalace aktualizací SW části probíhala pouze z důvěryhodných zdrojů (v souladu s projektovou dokumentací a dle postupů stanovených v provozních předpisech) a v souladu s platnými smluvními podmínkami výrobce daného SW (především s ohledem na licenční podmínky a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů).

V případě, že předmět plnění zahrnuje údržbu nebo vývoj softwaru, zavazuje se Poskytovatel:

1. Dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru definované na základě smluvního vztahu.
2. Pokud jsou softwarové auditní činnosti a předání zdrojového kódu k SW součástí plnění dle Smlouvy, umožní Poskytovatel Objednateli audit prováděného nebo provedeného plnění a na písemnou žádost Objednatele předloží Poskytovatel Objednateli vyvíjený zdrojový kód k SW na provedení codereview (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně), a to zejména za účelem ověření skutečnosti, zda Poskytovatel postupuje či postupoval při poskytování plnění v souladu se Smlouvou a těmito Bezpečnostními požadavky.
3. Poskytovat Objednateli v termínech stanovených Objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje softwaru či kdykoli po jeho předání.
4. Zajistit, že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování softwaru a/nebo které jsou specifikovány výslovně ve smlouvě (zejména, že software nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.).
5. Pokud je součástí plnění i instalace operačního systému případně softwaru třetích stran, zajistit v průběhu jeho instalace, že budou použity předepsané verze těchto produktů kompatibilní a funkční v prostředí Objednatele.
6. Zajistit bezpečnost testovacího prostředí u Poskytovatele a ochranu poskytnutých testovacích dat Objednatelem.
7. Zajistit, že v produkčním prostředí Objednatele bude dodán jen předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování předmětu plnění.
8. Zajistit, že v rámci poskytovaného plnění bude dodávaný software
9. v souladu s bezpečnostními politikami a standardy Objednatele
10. otestován na soulad s bezpečnostními politikami Objednatele (platí pro Poskytovatele, pokud byl s takovými bezpečnostními politikami seznámen)
11. Instalovat software pouze na základě Objednatelem předem schválených migračních postupů.
12. Předat zdrojový kód Objednateli bezpečnou formou zajištující jeho integritu.
13. Zajistit řízení verzí zdrojového kódu.
14. Zajistit zálohování zdrojového kódu a jeho uložení mimo produkční prostředí.
15. Zajistit, aby distribuce zdrojových kódů obsahovala soubor z vývojového prostředí na řízenou kompilaci těchto zdrojových kódů.
16. Nevyvíjet, nekompilovat a nešířit v prostředí Objednatele programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

### 2.6 Zvládání kybernetických bezpečnostních událostí a incidentů[[3]](#footnote-4)

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na dodržování, provozu a rozvoji bezpečnostních opatření Objednatele a zároveň se zavazuje:
2. Bez zbytečného odkladu hlásit Objednateli všechny bezpečnostní události a incidenty s potenciálním negativním dopadem na Objednatele, a to stanoveným komunikačním kanálem nebo prostřednictvím Kontaktní osoby.
3. Vyhodnocovat informace o bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.
4. V případě vzniku bezpečnostní události a následného zvládání a vyhodnocování bezpečnostního incidentu a/nebo v případě podezření na bezpečnostní incident poskytnout Objednateli součinnost a relevantní informace o podezřelém zařízení na straně Poskytovatele.
5. Bez zbytečného odkladu a po dohodě s Objednatelem realizovat opatření, požadovaná Objednatelem v dohodnutých termínech, ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování incidentu, který může mít dopad na Objednatele.
6. Spolupracovat při analýze příčin bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že poskytovatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.
7. Poskytovatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Bezpečnostních požadavků, jehož příčina je na straně Poskytovatele, nebude posuzován jako okolnost vylučující odpovědnost poskytovatele za prodlení s řádným a včasným plněním předmětu této smlouvy a nebude důvodem k jakékoli náhradě případné újmy poskytovateli či jiné osobě ze strany objednatele. Ostatní ustanovení ohledně odpovědnosti poskytovatele za prodlení obsažená v této smlouvě nejsou tímto ustanovením dotčena.

### 2.7 Řízení kontinuity činností

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na dodržování, provozu a rozvoji bezpečnostních opatření Objednatele a zároveň se zavazuje:
2. Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění.
3. Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně služeb.

### 2.8 Fyzická bezpečnost

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na dodržování, provozu a rozvoji bezpečnostních opatření Objednatele a zároveň se zavazuje:
2. Dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny komponenty systémů ICT, anebo datové nosiče.
3. V rozsahu předmětu plnění zajistit fyzické zabezpečení instalačních, záložních nebo archivních médií a dokumentace v souladu s Klasifikačním schématem, zejména označení, uchování a likvidaci. Fyzická likvidace použitých médií bude prováděna předepsanými postupy, kterými musí být garantováno zachování bezpečnostní klasifikace.

### 2.9 Bezpečnostní nástroje

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na dodržování, provozu a rozvoji bezpečnostních opatření Objednatele a zároveň se zavazuje:
2. Realizovat bezpečnostní opatření pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity komunikační sítě.
3. Realizovat přístup z mobilního zařízení do prostředí Objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN).
4. Připojovat do prostředí Objednatele pouze ta zařízení (switch, přístupový bod wifi, router, hub apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno oprávněnou osobu ve věcech technických na straně Objednatele určenou v této smlouvě.
5. Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, který je v rozsahu předmětu plnění a je ve správě Poskytovatele.
6. Na aktiva Objednatele neinstalovat a nepoužívat v prostředí Objednatele tyto typy nástrojů, pokud nejsou součástí předmětu plnění:
7. Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.
8. Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.
9. Analyzátor zranitelností (scanner zranitelností) – softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.
10. Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT.
11. Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí Objednatele.
12. Připojovat do prostředí Objednatele pouze zařízení ICT, která splňují tyto požadavky:
13. musí být aplikovány bezpečnostní záplaty (operačního systému, internetového prohlížeče a dále balíku MS Office, Javy a případně dalšího SW vybavení, pokud je používáno);
14. musí mít nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu.
15. Používaná paměťová média (flash disky, diskety, CD a DVD nosiče apod.), musí být před použitím zkontrolována v zařízení, které má nainstalovanou aktualizovanou antivirovou ochranu.
16. Musí být připojováno pouze do vyhrazené bezpečnostní zóny a způsobem definovaným v provozní nebo projektové dokumentaci. Pokud v provozní nebo projektové dokumentaci definováno není, předpokládá se, že se připojení takových zařízení nedovoluje.
17. Pokud je k údržbě používáno zařízení typu notebook/počítač, které není vyhrazené pouze pro účel údržby systému ICT objednatele, poté musí splňovat podmínky uvedené v této kapitole.
18. Průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné české a evropské legislativy.
19. Na vyžádání poskytnout Objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění, a to po celou dobu trvání smlouvy a do 2 let po jejím ukončení.
20. Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.
21. Pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran.
22. Veškeré neveřejné informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístup, a to zejména na mobilních zařízeních.
23. Poskytovatel bere na vědomí, že v případě, kdy technické spojení společnosti Koncernu ÚJV s Poskytovatelem narušuje chod služeb společnosti Koncernu ÚJV nebo Koncernu ČEZ, může být toto spojení ihned ukončeno bez předchozího upozornění, pokud smlouva nestanoví jinak.

Poskytovatel bere na vědomí, že veškeré aktivity Poskytovatele a jeho plnění realizované v prostředí Objednatele jsou monitorovány a vyhodnocovány v rozsahu předměty plnění a v souladu s interními dokumenty Objednatele, se kterými byl Poskytovatel seznámen.

1. pro změnu Kontaktní osoby pro bezpečnost na straně poskytovatele se užije ustanovení týkající se změny Oprávněných osob smluvních stran. Změnu Kontaktní osoby pro bezpečnost na straně poskytovatele je poskytovatel povinen nahlásit do 5 dnů od provedení změny. [↑](#footnote-ref-2)
2. Data a informace obsahující prvky extrémismu, terorismu, pornografie anebo podněcování k nesnášenlivosti a společenským předsudkům vztahujícím se ke společenské skupině identifikované na základě rasy, náboženství nebo víry, pohlaví, sexuální orientace, národnostní a etnické příslušnosti či jiné odlišnosti. [↑](#footnote-ref-3)
3. Pojem bezpečnostní incident a bezpečnostní událost je ekvivalentní pojmům Kybernetická bezpečnostní událost / Kybernetický bezpečnostní incident, vydefinovaných zákonem č. 181/2014 Sb. o kybernetické bezpečnosti, v platném znění. [↑](#footnote-ref-4)