Bezpečnostní požadavky pro dodávky standardních systémů a technologií

1 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, která má pracovněprávní či obdobný smluvní vztah s Poskytovatelem nebo jeho poddodavateli
Klasifikační schéma	Klasifikační schéma určující nakládání s daty a informacemi SKČ 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

2 Bezpečnostní opatření

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) zákona č. 181/2018, Sb., o kybernetické bezpečnosti a je povinen naplnit požadavky související legislativy.

2.1 Systém řízení bezpečnosti informací

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

a) 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.

b) Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění.

c) Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je a vyhodnocovat jejich účinnost.

d) 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.

e) Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.

f) 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.

g) Využívá-li při poskytování předmětu plnění poddodavatele, zajistit adekvátní dodržování těchto Bezpečnostních požadavků rovněž ve smluvních vztazích se svými poddodavateli.

h) 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

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

a) 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).

b) 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;

c) Dodržovat příslušná ustanovení interních řídicích aktů 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;

d) 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;

e) 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:

- Pro uložení a sdíleni dat a informací Objednatele využívaly pouze k tomu schválené prostředky;
- Neukládaly ani nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;
- Nestahovaly, nesdílely, neukládaly, nearchivovaly ani neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem;
- Nenavštěvovaly internetové stránky s eticky nevhodným obsahem;
- Nerealizovaly pokusy o neautorizovaný přístup ke zdrojům Objednatele ani ke zdrojům jiných subjektů;
- 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;
- Nepodílely se s prostředky Objednatele na šíření spamu ani škodlivého softwaru

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 Bezpečnost provozu a komunikací

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

a) Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění.

b) Na vyžádání poskytnout Objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.

c) 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

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

a) Přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele.

b) Zajistit, aby udělený přístup nebyl sdílen více osobami za stranu Poskytovatele.

c) 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).

d) Zajistit, aby osoby podílející se na poskytování předmětu plnění a mající přístup k informačním aktivum SKČ chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.

e) Průběžně kontrolovat a vyhodnocovat oprávněnost přístupu, jak fyzického, tak i logického, u všech osob na straně Poskytovatele, které přistupují do prostředí Objednatele.

V případě, že Poskytovatel přistupuje do systému ICT Objednatele:

i) 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 vygenerovaným jednoznačným identifikátorem, dále pak zaevidované v registru identit, a to na základě požadavku poskytovatele na přístup. Pro zaevidování v registru identit je nezbytné sdělení těchto osobních údajů zaměstnance Poskytovatele:

- Jméno (Registr identit)
- Příjmení (Registr identit)
- Rodné příjmení (Registr identit)
- Pohlaví (pouze při ověření, bez záznamu v registru identit)
- Datum narození (Registr identit)
- 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).
- Email (Registr identit)
- Mobilní telefon případně pevná linka (Registr identit)

j) Poskytovatel se zavazuje informovat své zaměstnance a poddodavatele, kterým bude přidělen přístup (fyzický, logický) k systému ICT, o způsobu zpracování jejich osobních údajů.

k) Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci poskytovatele musí být řízeno principem nezbytného minima a není nárokové.

l) 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

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

a) Zajistit bezpečnou implementaci, inovaci, aktualizaci, testování technologií, které jsou předmětem plnění.

b) Předat Objednateli dokumentaci předmětu plnění minimálně v následujícím rozsahu:

- dokumentaci skutečného provedení
- dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů
- dokumentaci obsahující popis autorizačního konceptu a oprávnění
- dokumentaci obsahující zálohovací a archivační postupy
- dokumentaci obsahující instalační a konfigurační postupy
- dokumentaci pro zajištění kontinuity provozu a obnovy po havárii

2.5.1 Vývoj softwaru

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

a) Dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru definované na základě smluvního vztahu.

b) 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.

c) 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.

d) 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.).

e) 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.

f) Zajistit bezpečnost testovacího prostředí u Poskytovatele a ochranu poskytnutých testovacích dat Objednatelem.

g) Zajistit, že v produkčním prostředí Objednatele bude dodán jen předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování předmětu plnění.

h) Zajistit, že v rámci poskytovaného plnění bude dodávaný software

- v souladu s bezpečnostními politikami a standardy Objednatele
- otestován na soulad s bezpečnostními politikami Objednatele (platí pro Poskytovatele, pokud byl s takovými bezpečnostními politikami seznámen)

i) Instalovat software pouze na základě Objednatelem předem schválených migračních postupů.

j) Předat zdrojový kód Objednateli bezpečnou formou zajišťující jeho integritu.

k) Zajistit řízení verzí zdrojového kódu.

l) Zajistit zálohování zdrojového kódu a jeho uložení mimo produkční prostředí.

m) Zajistit, aby distribuce zdrojových kódů obsahovala soubor z vývojového prostředí na řízenou kompilaci těchto zdrojových kódů.

n) 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

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

a) 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.

b) Vyhodnocovat informace o bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.

c) 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.

d) 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.

e) 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.

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

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

a) Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění.

b) Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně služeb.

2.8 Fyzická bezpečnost

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

a) 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.
b) V rozsahu předmětu plnění zajistit fyzické zabezpečení instalačních, záložních nebo archivních médií a dokumentace v souladu s Klasifikačním schématem, zejména označení, uchování a likvidaci.

2.9 Bezpečnostní nástroje

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

a) Realizovat bezpečnostní opatření pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity komunikační sítě.
b) Realizovat přístup z mobilního zařízení do prostředí Objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN).
c) 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.
d) 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.
e) Na aktiva Objednatele neinstalovat a nepoužívat v prostředí Objednatele tyto typy nástrojů, pokud nejsou součástí předmětu plnění:.
    - Keylogger - software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.
    - Sniffer - software nebo hardware umožňující odposlouchávání síťového provozu.
    - 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.
    - Backdoor - skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT.
    - Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí Objednatele.
f) Připojovat do prostředí Objednatele pouze zařízení ICT, která splňují tyto požadavky:
    - musí být aplikovány bezpečnostní záplaty (operačního systému, internetového prohlížeče a dále balíku MS Office, Javy a případně dalšího SW vybavení, pokud je používáno);
    - musí mít nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu.
    - Používaná paměťová média (flash disky, diskety, CD a DVD nosiče, apod.), musí být před

použitím zkontrolována v zařízení, které má nainstalovanou aktualizovanou antivirovou ochranu.

- 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.

g) 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.

h) 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.

i) Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.

j) Pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran.

k) Veškeré neveřejné informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístup, a to zejména na mobilních zařízeních.

Poskytovatel bere na vědomí, že v případě, kdy technické spojení společnosti Koncernu ÚJV s Poskytovatelem narušuje chod služeb společnosti Koncernu ÚJV, 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 předmětu plnění a v souladu s interními dokumenty Objednatele, se kterými byl Poskytovatel seznámen