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 a mající 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

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. 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, 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

1. 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.

2. 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:

   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

1. 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.

2. Poskytovatel bere na vědomí, že přístup k systému ICT je možné povolit pouze fyzické identitě zaměstnance poskytovatele / poddodavatele poskytovatele s vygenerovaným jednoznačným identifikátorem IPD, dále pak zaevidované v registru identit SKČ, a to na základě požadavku poskytovatele na přístup. Pro zaevidování v registru identit Skupiny ČEZ je nezbytné sdělení těchto osobních údajů zaměstnance Poskytovatele:
   - Jméno (Registr identit, Generátor IPD)
   - Příjmení (Registr identit, Generátor IPD)
   - Rodné příjmení (Registr identit, Generátor IPD)
   - Pohlaví (Generátor IPD)
   - Datum narození (Registr identit, Generátor IPD)
   - Rodné číslo (Generátor IPD – ŘČ v systémech neukládáme, nepožadujeme jeho zasílání ani zaznamenání do formuláře ale je vyžadováno při generování identifikátoru IPD, kdy toto fyzická identita sdělí v okamžiku generování jednoznačného identifikátoru IPD. V případě nesouhlasu fyzické osoby s použitím RČ je IPD generováno z data narození a dalších osobních údajů fyzické osoby).
   - Email (Registr identit, Generátor IPD)
   - Mobilní telefon případně pevná linka (Registr identit)
3. 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.
4. Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci poskytovatele musí být řízeno principem nezbytného minima a není nárokové.
5. 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 SKČ).

2.5 Akvizice, vývoj a údržba

1. 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. 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

1. 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.
2. 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:
   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

1. 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

1. 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.

2. Poskytovatel bere na vědomí, že v případě, kdy technické spojení společnosti Koncernu ČEZ s Poskytovatelem narušuje chod služeb společnosti Koncernu ČEZ, může být toto spojení ihned ukončeno bez předchozího upozornění, pokud smlouva nestanoví jinak.

3. 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.

Security requirements for delivering standard systems and technologies

1 INTRODUCTORY PROVISIONS

For the purpose of this attachment to the Agreement, the following abbreviations and terms are used:

Act or CSA	Act No. 181/2014 Coll., concerning Cyber security and change of related laws (Cyber Security Act), in the wording of later regulations
CSD	Decree No. 82/2018 Coll. on security measures, cybersecurity incidents, reactive measures, particulars of filings concerning cybersecurity, and disposal of data (Cybersecurity Decree), as amended.
Regulation	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation)
Personal information	All information about an identified or identifiable physical person (such as name, identification number, location data, network identifier, or one or more specific physical, physiological, genetic, economic, cultural or social identity of that individual).
Personal information processing	Any operation or set of operations that is performed with personal data or personal data files, such as collecting, recording, organizing, structuring, storing, customizing or modifying, retrieving, viewing, using, making available through transmission, dissemination or any other disclosure, alignment or combination, restriction, erasure or destruction.
Date of the agreement conclusion	Date of the conclusion of this agreement or the date of integration of said Security requirements into the agreement through the appendix of this agreement.
Individual prom the Provider's party	A physical individual participating in the fulfillment of the contract and having a labor or similar contract relationship with the Provider or their sub-providers
Classification scheme	Classification scheme specifying handling data and information of CEZ Group in paper and electronic form.
Consumer's environment	Physical perimeter specified by the physical space in rent or property of the Consumer or a logical perimeter defined by the network elements in the administration or the property of the Consumer.

2 SECURITY MEASURES

2.1 System of Management of Information Security

1. The Provider acknowledges, that the Consumer has_established the Information Security Management System according to ISO/IEC 27001 and is a person according to § 3 paragraph c) and d), eventually f) or g) of the Act 181/2018 Coll. and is bound to fulfill the requirements of the related legislation.
2. The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at a minimum, bound to:

   a) Procure security principles and processes, which will cover the security of data and information, that can be created and processed on by the Consumer party under the terms and conditions of the contract.
   b) Manage their own risks that can affect the provision of the terms and conditions of the contract.
   c) Based on the security requirements and results of risk evaluation, implement appropriate security measures according to the terms and conditions of the contract, monitor them, and evaluate their efficiency.
   d) Keep a record of the security policy covering security of data and information, which can be created and processed by the Consumer's party under the terms and conditions of the contract. The security policy must include the general principles, objectives, security requirements, rights and obligations concerning the management of information security.
   e) Set up and maintain the current security measure in the form of processes and technologies, ensuring fulfillment of the security policy.
   f) Keep a record of the creation and processing of data and information according to the provided terms and conditions of the contract, record all significant circumstances concerning the assurance of the security of the data and information and grant access to them upon the request of the Consumer.
   g) In case of using a sub-contractor, ensure inclusion of adequate compliance to Security requirements in contract relationships with their sub-contractors.
   h) After the contract performance termination, without undue delay, shred all Information and data of the Consumer, which were handed over during the performance of the contract.

2.2 Human Resources Security

1. The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at a minimum, bound to:
   a) Ensure the person responsible in contract terms, within 10 days of entering the contract, confirms, in written form, to the Consumer, that all individuals participating in the fulfillment of the terms and conditions of the contract for the Provider's party are provably introduced to the security requirements and rules of CYBEX (Cyber security rules for external employees).
   b) Provide the terms and conditions of the contract employing only Authorized individuals, which have been properly introduced to the rules of CYBEX and possess verified

qualification, knowledge and experience according to the terms and conditions of the contract.

c) Adhere to relative provisions control Acts of CEZ Group in the extent in which they have been introduced to said Acts. The provable introduction is deemed as the Provider's employee training provided by the Consumer, electronic transfer or transfer by protocol of the relative documentation or access to a shared repository, provided by the Consumer, containing relative internal control Act.

d) In case a supervision over the terms and conditions of the contract service is part of the terms and conditions of the contract, define and fulfill roles and accountability for monitoring networks and devices according to the terms and conditions of the contract.

e) Ensure, that individuals participating in fulfillment of the terms and conditions of the contract for the Consumer in Consumer's environment or with Consumer's assets, including the case the Consumer's assets are used outside of Consumers environment:
   - For saving and sharing data and information of the Consumer using only approved media;
   - Not saving or sharing data and information with ethically inappropriate content conflicting with good behavior or damaging the name of the Consumer;
   - Not downloading, sharing, saving, archiving, or installing data files and executable files conflicting with the terms and conditions of the license or copyright;
   - Not visiting web pages with ethically inappropriate content;
   - Not attempting unauthorized access to the resources of the Consumer or other subjects;
   - Not attempting unauthorized modification or other unauthorized interference with resources of the Consumer, not even in the case, that the resource of the Consumer is managed by them;
   - Not participating with the resources of the Consumer in spreading spam or malicious software.

2. The provider acknowledges that part of the conditions, in order to gain access to Consumer's resources, is processing of Provider's employees' personal information, of those who participate in the fulfillment of the terms and conditions of the contract, by the Consumer. In case the Consumer is not enabled to process personal information of the affected employees, said employees will not be granted access to the resources of the Consumer.

2.3 Management of Operation and Communications

1. The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at a minimum, bound to:

   a) Ensure safe operation of the information system and the infrastructure used for fulfillment the terms and conditions of the contract.

   b) On request, provide a summary, report, or other adequate information concerning the security measures implemented in their information system and infrastructure.

   c) Ensure that, for fulfillment of the terms and conditions of the contract only applications and technologies are used that are in accordance with valid Czech and European legislation and, in particular, with the license conditions of the Act No. 121/2000 Coll., concerning copyright, as well as those concerning the laws related to copyright and related amendments.

2.4 Management of Approach and Secure User Behavior

1. The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at a minimum, bound to:

   a) Assign authorization to their individual employees to carry out actions in such a way that the risk of undesired access to the Consumer's assets is minimized.
   b) Ensure, that granted access is not shared by several individuals in the Producer's party.
   c) State in the request for access the extent of data/information, service, purpose, for which is the access to the ICT system of the Consumer requested and a time specification of the duration of the validity of the access (e.g.: for an indefinite period / 1 year / 1 month / 1 day).
   d) Ensure that individuals participating in the fulfillment of the terms and conditions of the contract, who have access to the information asset of CEZ Group, keep the authentication media and information safe, and under no circumstances provide unauthorized access to other individuals.
   e) Continuously control and evaluate the validity and necessity of access, both physical and logical, of all individuals from the Provider's party that enter the Consumer's environment.

2. The Provider acknowledges, that the access to the ICT system is possible to allow only to the physical persons identified as an employee of the Provider / Provider's sub-contractor with the generated unique IPD identifier and registered in the registry of CEZ Group identities only on basis of a Provider's request for access. In order to register in the CEZ Group Identity Register, it is necessary to disclose these personal data to the Provider's employee:
   - Name (Identity Register, IPD Generator)
   - Last Name (Identity Register, IPD Generator)
   - Maiden name (Identity Register, IPD Generator)
   - Gender (IPD Generator)
   - Birth Date (Identity Register, IPD Generator)
   - Personal Identification Number (IPD Generator does not store PIN in the system, we do not require it to be sent or recorded in the form, but it is required to generate the IPD identifier, physical identity communicates it at the time of generating a unique IPD. In case of persons disagreement, the IPD is generated from the date of birth and other personal data).
   - Email (Identity Register, IPD Generator)
   - Mobile phone or landline (Identity Register)
3. The Provider acknowledges informing its employees and subcontractors to whom the access (physical, logical) to the ICT system will be assigned, the manner of processing their personal data, and the Provide undertakes to process personal data exclusively in accordance with the Regulation.
4. The Provider acknowledges that authorization assigning to the Provider's employee must be controlled by the principle of minimum necessity and is not claimable.
5. The Provider acknowledges that in case of unsuccessful attempts to authorize a user (an individual from Provider's party), the respective account can be blocked and treated as a security incident and measures for security incident management can be applied (e.g.: immediate cancellation of access to the information assets of CEZ Group).

2.5 Acquisition, Development and Maintenance

1. The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at a minimum, bound to:

   a) Ensure secure implementation, innovation, update and testing of technologies that are part of the terms and conditions of the contract.

   b) Transfer the documentation of the terms and conditions of the contract to the Consumer including at least:
      - documentation of actual execution
      - documentation of all security settings, functions and mechanisms
      - documentation including a description of authorization concept and authority
      - documentation including back-up and archiving processes
      - documentation including installation and configuration processes
      - documentation for ensuring the continuity of operation and recovery after an accident

2. In case the terms and conditions of the contract include software development, the Provider is bound to:

   a) Adhere to and implement the best practices for safe software development defined in the contract relationship.

   b) Allow the Consumer to carry out an audit on the fulfillment of the contract and, on written request, present the Consumer with developed sources code of software, if the audit activities and showing the source code are mentioned in the contract. The consumer will be allowed to execute code review (automated through security tools, and manual), especially in order to verify that the Provider is proceeding or proceeded in fulfilling the contract according to the terms and conditions of the contract and the Security requirements.

   c) Provide the Consumer, in the terms stated by the Consumer, respectively, without unnecessary delay, the requested co-operation on execution of security testing during the development of the software or anytime after the delivery of the software.

   d) Ensure that the fulfillment will include only the elements that are objectively necessary for proper operation of the software and/or that are explicitly specified in the contract (especially that the software will not include any unnecessary components, any program samples etc.).

   e) In case the installation of the operating system or other third-party software is a part of the fulfillment of the contract, ensure, during its installation, that the specified versions of these products installed are compatible and functional within the Consumer's environment.

   f) Ensure the security of the Provider's testing environment and security of the testing data provided by the Consumer.

   g) Ensure that only an executable code, specified by the terms and conditions of the contract will be supplied within the production environment, and the necessary data for operation of the contract fulfillment will be compiled.

   h) Ensure that, according to the terms and conditions of the contract, the provided software will be
      - in accordance with the security policies and standards of the Consumer
      - tested in accordance with the security policies of the Consumer (applies to the Provider, in case they were introduced to such security policies)

i) Install software only based on the migration processes approved by the Consumer in advance.
j) Transfer the source code to the Consumer in secure form, ensuring its integrity.
k) Ensure the management of various versions of the source code.
l) Ensure the back-up of the source code and its safe storage outside the production environment.
m) Ensure that the distribution of the source code includes a file from the development environment for directed compilation of said source codes.
n) Not develop, compile or share, in the environment of the Consumer, a program code with the purpose of illegal takeover, disruption of access, confidentiality or integrity or unauthorized and illegal acquisition of data and information.

2.6 Cyber Security Events and Incidents Management

1. The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at a minimum, bound to:

   a) Without unnecessary delay, report to the Consumer all security events and incidents with potential negative impact to the Consumer through a specified communication channel or through the Contact Person.
   b) Evaluate concerning information security incidents and preserve it for future use according to the requirements of valid Czech and European legislation.
   c) In case of a security event and consecutive management and evaluation of the security incident, and/or in case of suspicion of a security incident, provide the Consumer with the relevant information concerning an identified suspicious device or individual from the Provider's party.
   d) Without unnecessary delay, and after agreement with the Consumer, implement measures requested by the Consumer within the agreed terms in order to reduce the impact of a security incident or prevent the continuation of an incident, that can make an impact to the Customer.
   e) Co-operate in the analysis of the causes of security incident and suggest measures with the intention to prevent its recurrence in case the security incident was cause by the Provider, or the Provider participated in its origin.

2. The Provider acknowledges that the process of management of security incidents, or other consequential breach of the Security Requirements, caused by the Provider will not be considered as a circumstance excluding the responsibility of the Provider for delaying the fulfillment of the terms and conditions of the contract and will not be a basis for a compensation of any kind in case of damage to the Provider or any other individual from the Consumer's party. Other provisions concerning the accountability of the Provider for extensions included in the contract are not influenced by the provision.

2.7 Business Continuity Management

1. The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at a minimum, bound to:

a) Ensure adequate continuity of any assets in their ownership that are necessary for the fulfillment of the terms and conditions of the contract.
b) Continuously control and test that they are capable of ensuring the continuity of assets according to the agreed level of service.

2.8 Physical Security

1. The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at a minimum, bound to:
   a) Adhere to the operational rules of the buildings (regime measures) and used spaces, especially in the area of physical safety of security areas, where the components of ICT systems or the data carriers are placed.
   b) In accordance with the terms and conditions of the contract, ensure the physical safety of the installation, back-up or archiving of media and documentation in accordance with the Classification scheme, especially labeling, preservation and disposal.

2.9 Security Tools

1. The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at a minimum, bound to:

   a) Implement security measures for removal or blockage of the network connection/connections that does/do not fulfill the requirements for the security of the integrity of the communication network.
   b) Implement access from a mobile device to the environment of the Consumer only through secured connection of virtual private network (VPN).
   c) Connect to the environment of the Consumer only such devices (switch, Wi-Fi access point, router, hub etc.) that have passed through an approval process, including that their connection was approved by an authorized individual in technical matters from the Consumer's party, and who is identified in the contract.
   d) Without unnecessary delay, document and deactivate all unused terminals in the network or unused ports in active network element, that is according to the terms and conditions of the contract and is in the report of the Provider.
   e) Avoid installation onto any assets of the Consumer, or use in the environment of the Consumer, the following types of tools, unless they are part of the contract:
      - Keylogger – software or hardware, that can, without authorization, log keystrokes with the aim to disrupt the confidentiality of the input data and information.
      - Sniffer – software or hardware, that allows unauthorized monitoring of network traffic.
      - Weakness analyzer (Weakness scanner) – software or hardware tool allowing the search and identification of weaknesses in the ICT systems, detection of available network services and ports, running processes, running afflictions and their versions etc.
      - Backdoor – hidden software or hardware tool, allowing bypass of approved authentication procedures, installed with the aim of providing easy, unauthorized access to the ICT system.
      - Malware and other malicious software that disturbs bypasses or restricts the security measures in the Consumer environment in any way.

f) connect to the Consumer environment only ICT devices that meets the following requirements:
   - Security patches must be applied (operating system, internet browser, MS Office, Java and possibly other SW if applicable);
   - Must have anti-virus protection installed, running, and updated.
   - The mass storage media (flash drives, floppy disks, CDs, and DVDs, etc.) must be checked on a device that has updated antivirus protection before it can be used.
   - It must be connected only to dedicated secure zone as defined in the operations or project documentation. If it is not defined in the operations or project documentation, it is assumed that the connection of such devices is not permitted.

g) Continuously record and preserve data concerning the ICT device operation (operation and localization information) according to the contract and in adherence with requirements of valid Czech and European legislation.

h) Upon request, provide the Consumer with a report including the results of monitoring of all user and administrative activities and other events according to the contract and for up to 2 years after the termination of the contract.

i) Ensure the collection of information concerning the operational and security activities according to the contract, and the security of acquired information from unauthorized reading or modification.

j) For on-line transactions completed through web technologies, implement TLS/SSL certificates with the aim of ensuring their confidentiality, integrity and identity communicating parties.

k) Secure all private information provided by the Consumer with appropriate encryption and against unauthorized access, especially on the mobile devices.

2. The Provider acknowledges that, if the technical connection of the CEZ Group to the Provider is causing disturbance to the functioning of the CEZ Group, the connection can immediately be ended without prior warning, unless the contract states otherwise.

3. The Provider acknowledges that all activities of the Provider and their fulfillment realized in the environment of the Consumer are monitored and evaluated in accordance with the fulfillment of the contract and adheres to the internal documents of the Consumer, which have been introduced to the Provider.