Bezpečnostní požadavky pro poskytovatele konzultační a poradenské činnosti

1. Účel

a) Definovat bezpečnostní požadavky pro Poskytovatele konzultační a poradenské činnosti, kdy v této souvislosti Poskytovatel přistupuje k informacím Objednatele. Využívá-li Poskytovatel při poskytování předmětu plnění poddodavatele, je povinen zajistit adekvátní dodržování těchto Bezpečnostních požadavků rovněž ve smluvních vztazích se svými poddodavateli.
b) Zajistit ochranu informací Objednatele, se kterými se Poskytoval seznámí v rámci jednání a následném plnění smlouvy.

2. Bezpečnostní požadavky

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.
e) Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.
f) Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění.
g) Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.
h) Na vyžádání poskytnout Objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.

2.2. Přístup k informacím Objednatele

Veškeré zpřístupněné informace zůstávají výhradním vlastnictvím Objednatele a Poskytovatel je oprávněn tyto informace užít jen pro účely plnění smlouvy Objednavatele.

Poskytovatel se zavazuje:

a) sdělit informace Objednatele pouze těm svým zaměstnancům nebo spolupracujícím osobám, které nezbytně informace potřebují znát pro účely plnění této smlouvy, jsou současně zavázáni k mlčenlivosti a byli seznámeni s těmito Bezpečnostními požadavky;

b) nezneužít informace Objednatele k jinému účelu, než je plnění předmětu smlouvy, zejména nenakládat s informacemi v rozporu s oprávněnými zájmy Objednatele;

c) zabezpečit informace Objednatele před jejím zpřístupněním nepovoleným třetím osobám, a to přijetím potřebných technickoorganizační opatření, která zamezí neoprávněnému nebo nahodilému přístupu k informacím Objednatele, k jejich zničení či ztrátě, nebo neoprávněnému užití ze strany nepovolené osoby;

d) pořizovat kopie informací Objednatele pouze v nezbytných případech;

e) veškeré informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístup, a to zejména na mobilních zařízeních.

f) po skončení plnění smlouvy bez zbytečného odkladu skartovat veškeré informace a data Objednatele, které mu byly v souvislosti s plněním smlouvy předány.

V případě, že Poskytovatel přistupuje do systému ICT Objednatele:

g) 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)

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

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

j) 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).

2.3. Bezpečnost přenosu dat a informací

K účelům přenosu dat a informací musí být na obou stranách určena (jmenována) Kontaktní osoba, která je autorizována přenos dat a informací provádět. Bezpečné možnosti přenosu dat a informací jsou:

a) Šifrovaná emailová komunikace (MIP, S/MIME nebo zip s heslem)
b) Externí SharePoint (EDP) – služba poskytovaná společností ČEZ ICT Services, a.s.
c) Šifrované přenosné zařízení zabezpečené PINem (USB disk)
d) Předání tištěných informací (osobně / poštou)
e) Datová schránka
f) Portál dodavatele

2.4. Zvládání bezpečnostních událostí a incidentů

Poskytovatel 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) 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.
c) 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.
d) 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.

Security requirements for Providers of consulting and advisory services

1. Purpose

a) Define the Security Requirements for providers of consulting and advisory services, if the Provider accesses the Consumer´s Information within this context. If the Provider uses a subcontractor in providing the subject of performance, it is obliged to ensure adequate compliance with these Security Requirements also in contractual relations with its subcontractors.
b) Assure Consumer´s information security, with which the Provider becomes acquainted during the negotiations and subsequent performance of the contract.

2. Security Requirements

The Provider acknowledges, that the Consumer has established the Information Security Management System according to ISO/IEC 27001 and is a subject according to § 3 paragraph c) and d), eventually f) and g) of the Act 181/2018 Coll. and is obliged to meet the requirements of the related legislation.

2.1. Information Security Management System

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

a) Implement security principles and processes, which will cover the data and information security, that can be created and processed on by the Consumer when providing the subject of performance.
b) Manage their own risks that can affect the provision of the subject of performance.
c) Based on security needs and risk evaluation results, implement appropriate security measures within the scope of the provided subject of performance, monitor them and evaluate their effectiveness.
d) Create and approve a security policy that will cover the data and information security that may be created and processed by the Provider in providing the subject of performance.
e) Establish and maintain current security measures in the form of processes and technological means that ensure compliance with the security policy.
f) Ensure the safe operation of the information system and infrastructure used to provide the subject of performance.
g) Ensure the collection of information on operational and safety activities within the scope of the subject of performance and the protection of the information obtained against its unauthorized reading or change.
h) Upon request, provide the Consumer with an overview, report or other adequate information on security measures implemented in its information system and infrastructure.

2.2. Access to Consumer´s information

All available information remains the Consumer property and the Provider is entitled to use this information only for the purposes of fulfilling the subject of performance.

The Provider is, at least, bound to:

- **a)** Communicate the Consumer´s information only to their employees or cooperating persons who necessarily need to know the information for the purposes of performance of this contract, are simultaneously bound to confidentiality and have been acquainted with these security requirements.
- **b)** Not to misuse the Consumer´s information for a purpose other than the subject of performance, not to handle information contrary to the Consumer´s legitimate interests.
- **c)** Secure the Consumer´s information against the access of unauthorized third parties by taking the necessary technical and organizational measures to prevent unauthorized or accidental access to the Consumer´s information, its destruction or loss, or unauthorized usage.
- **d)** Make copies of the Consumer´s information only in necessary cases.
- **e)** Protect all information provided by the Consumer by appropriate encryption and against unauthorized access, especially on mobile devices.
- **f)** After the termination of the performance of the contract, without undue delay, dissolve all Consumer´s information and data which were handed over in connection with performance of the contract.

In case when Provider accesses the Consumer´s ICT system:

- **g)** The Provider acknowledges, that the access to the ICT system can be allowed only to the physical identity of the Provider´s / subcontractor´s employee with the generated unique IPD identifier and registered in the registry of CEZ Group identities, based on the Provider´s request for access. For registration 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)
  - Date of birth (Identity register, IPD generator)
  - Birth number (IPD generator – it is not stored, it´s not required to be sent or recorded in the form, but it´s required to generate the identifier. Person discloses it at the time of generating; valid only for Czech citizens. 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 (IPD register)
- **h)** The Provider acknowledges informing the employees and subcontractors, to whom the access (physical, logical) to the ICT system will be assigned, the manner of processing their personal data.
- **i)** The Provider acknowledges that authorization assigning to the Provider´s employee must be controlled by the principle of least privilege and is not claimable.
- **j)** 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).

2.3. Security of data and information transfer

For the purposes of data and information transfer, a Contact Person must be assigned (appointed) on both sides, who is authorized to perform data and information transfer. Secure data and information transfer options are:

- **a)** Encrypted email communication (MIP, S/MIME or zip with password);
- **b)** External SharePoint – service provided by ČEZ ICT Services;
- **c)** Encrypted portable device secured by PIN (USB flash disc);
- **d)** Transmission of printed information (in person / by mail);
- **e)** Data box;
- **f)** Supplier´s portal.

2.4. Security Events and Incidents Management

The Provider is, at least, bound to:

- **a)** Without unnecessary delay, report all security events and incidents with potential negative impact to the Consumer through a specified communication channel or through the Contact Person.
- **b)** In case of security event and following treatment 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.
- **c)** 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 the incident, that can make an impact to the Customer.
- **d)** 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 caused by the Provider, or the Provider participated in its origin.

The Provider acknowledges that the process of security incidents management, 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.