**Příloha 9b - Technicko-organizační opatření bezpečnosti informací a ochrany osobních údajů**

**Název stavby: TR Blansko – rozš. R110kV, doplnění T103**

1. **Požadavky na bezpečnost informací**

Všeobecné požadavky, které se vztahují obecně na poskytování všech Služeb Zhotovitelem.

* 1. **Důvěryhodná dodávka**: Zhotovitel zajistí, aby jím používané hardwarové a softwarové produkty byly nakupovány ze známých a spolehlivých zdrojů a aby byla zajištěna spolehlivá technická podpora a identifikovatelný dodavatelský řetězec.
  2. **Správa bezpečnosti informací**: Zhotovitel zavede, udržuje a sleduje rámec řízení bezpečnosti informací. Ten umožňuje vedení společnosti Zhotovitele stanovit jasné směřování a cíle v oblasti bezpečnosti informací a řízení rizik. Tím vedení společnosti Zhotovitele dává najevo závazek s naplňováním těchto cílů.
  3. **Řízení rizika v oblasti bezpečnosti informací**: Zhotovitel zajistí, aby (i) před zavedením nových IT systémů, ve kterých jsou zpracovávány informace společnosti E.ON, (ii) před zavedením významných změn ve stávajících systémech (iii) před zavedením významných nových technologií, byla zjištěna, hodnocena, řešena, sledována a udržována související rizika v přijatelných mezích pro oblasti bezpečnosti informací. Zhotovitel bez zbytečného odkladu poskytne na vyžádání společnosti E.ON informace týkající se činností ve vztahu k procesu řízení rizik.
  4. **Řízení bezpečnosti**: Zhotovitel (i) zřídil specializovanou roli pro bezpečnost informací, která je na dostatečně vysoké úrovni řízení se svěřenými přiměřenými pravomocemi i zdroji k zajištění účinného a důsledného uplatňování osvědčených postupů v oblasti bezpečnosti informací v celé společnosti a dodržování právních, regulačních a smluvních požadavků, které se týkají bezpečnosti informací. Zhotovitel (ii) realizuje komplexní, průběžný program zvyšování bezpečnostního povědomí s cílem propagovat žádoucí chování v oblasti bezpečnosti ve vztahu ke všem osobám, které mají přístup k informacím společnosti E.ON, a toto chování jim vštěpovat.
  5. **Zdokumentované provozní postupy**: Zhotovitel stanovil odpovědnosti a postupy pro řízení a provozování svých Služeb s cílem zajistit, aby po dobu trvání této smlouvy tato dokumentace byla (i) v souladu s uznávanými oborovými normami a osvědčenými postupy, (ii) řádně písemně vyhotovena a (iii) průběžně aktualizována. Zhotovitel bez zbytečného odkladu poskytne na vyžádání společnosti E.ON dokumentaci provozních postupů.
  6. **Správa aktiv**: Zhotovitel zajistí, aby (i) aktiva (hardwarové a softwarové prostředky), která se používají k vytváření, zpracování, ukládání nebo předávání informací společnosti E.ON, byla během celého životního cyklu chráněna proti poškození, ztrátě, krádeži a neoprávněnému zpřístupnění. Zhotovitel zajistí, aby tato aktiva byla evidována v inventáři aktiv, který (ii) je chráněn proti neoprávněnému pozměňování, (iii) aktualizován, (iv) pravidelně zálohován (v) a obsahuje potřebné údaje o těchto hardwarových a softwarových aktivech a případně – požadavky na dodržování předpisů v souvislosti s těmito aktivy. Zhotovitel zajistí, aby (vi) každému aktivu byl přiřazen jeho vlastník, který je odpovědný za provozování daného aktiva.
  7. **Řízení přístupu**: Zhotovitel omezí přístup k aktivům, která slouží k vytváření, zpracování, ukládání nebo předávání informací společnosti E.ON, na oprávněné osoby a pro vyhrazené provozní činnosti. To přinejmenším znamená, že (i) přístup k příslušným informacím mohou získat pouze oprávnění uživatelé, (ii) přístupová oprávnění jsou omezena na schválenou funkčnost systému, (iii) existuje jasné určení zodpovědnosti, (iv) přístupová oprávnění jsou udělována jednotlivcům (ID uživatele a hesla nesmějí být sdíleny). Zhotovitel zajistí, aby přístup pro správu k systémům, které slouží k ukládání nebo zpracování informací společnosti E.ON, byl (v) omezen na minimální počet správců, (vi) chráněn dvoufaktorovou autentizací, nebo pokud není možné dvoufaktorovou autentizaci technicky implementovat, zajistí obdobnou úroveň bezpečnosti řízení přístupu (jako jsou generovaná dočasná hesla v systémech pro správu, vynucování politiky hesel, použití kryptografických klíčů). Zhotovitel dále zajistí, aby byl přístup pro správu (vii) vždy protokolován s cílem umožnit zjištění a přešetření neoprávněného přístupu k informacím společnosti E.ON a neoprávněné manipulace s nimi. (viii) Zhotovitel rovněž zajistí, aby byl zaveden a dodržován formální postup, který definuje, jak jsou vytvářeny, pravidelně kontrolovány, upravovány, uzamykány a odstraňovány role, účty, přístupová práva a oprávnění týkající se přístupu.
  8. **Správa systémů**: Zhotovitel provozuje systémy, které vytvářejí, ukládají, zpracovávají nebo předávají informace společnosti E.ON takovým způsobem, aby (i) bylo možné zvládnout aktuální i předpokládanou pracovní zátěž a (ii) byly důsledně a přesně nakonfigurovány s cílem chránit tyto systémy a informace, které zpracovávají, ukládají nebo předávají, proti selhání, kybernetickému útoku, neoprávněnému zpřístupnění, poškození, krádeži či ztrátě. Zhotovitel zajišťuje správu zabezpečení systémů (iii) zálohováním nezbytných informací a softwaru, (iv) důsledným uplatňováním procesu provádění změn a (v) sledováním dodržování sjednaných dohod o úrovni služeb.
  9. **Síť a komunikace**: Zhotovitel zajistí, aby fyzické, bezdrátové a případně i hlasové sítě byly navrženy takovým způsobem, aby (i) byly spolehlivé a odolné, (ii) zabránily neoprávněnému přístupu, (iii) využívaly šifrované spojení a (iv) odhalily podezřelý provoz v síti. (v) Zhotovitel zajistí nakonfigurování síťových zařízení (včetně směrovačů, firewallů a bezdrátových přístupových bodů) tak, aby fungovaly podle potřeby a zabránily neoprávněným a nesprávným aktualizacím. Zhotovitel zajistí ochranu elektronických komunikačních systémů (vi) stanovením zásad pro jejich používání, (vii) nakonfigurováním bezpečnostního nastavení, (viii) posílením bezpečnostního nastavení podpůrné technické infrastruktury. (ix) Zhotovitel zajistí, aby názvy a topologie počítačů a sítí zůstaly skryty externím subjektům. Zhotovitel zajistí omezení externího přístupu k informačním systémům a sítím (x) zřízením demilitarizovaných zón (DMZ) mezi nedůvěryhodnými sítěmi a interními sítěmi, (xi) směrováním síťového provozu prostřednictvím firewallů nebo proxy firewallů, (xii) omezením způsobů připojení na nezbytné minimum(xiii) poskytnutím přístupu výhradně k autorizovaným podnikovým aplikacím, informačním systémům nebo konkrétně určeným částem sítě.
  10. **Správa technických bezpečnostních opatření**: Zhotovitel instaluje řešení ochrany proti škodlivému kódu v systémech, ve kterých mohou být informace společnosti E.ON vystaveny škodlivému kódu, včetně (i) serverů (např. aplikační servery, databázové servery, souborové servery, tiskové servery, webové servery), (ii) výpočetních zařízení (např. stolní počítače, notebooky a další mobilní zařízení) a iii) kancelářských zařízení (např. síťové tiskárny, kopírky, multifunkční zařízení). (iv) Software pro ochranu proti škodlivému kódu by měl chránit proti všem formám škodlivého kódu (např. viry, červy, trojské koně, spyware, rootkity, botnetový software, keyloggery, ransomware). (v) Software pro ochranu proti škodlivému kódu by měl být distribuován automaticky a v určených časových intervalech. Zhotovitel zjišťuje a pravidelně kontroluje, zda (vi) software pro ochranu proti škodlivému kódu nebyl deaktivován nebo zda jeho funkčnost nebyla omezena (vii) software pro ochranu proti škodlivému kódu správně nakonfigurovaný, (viii) jsou správně aplikovány aktualizace v rámci definovaných časových intervalů, (ix) probíhají kontroly systému v předem určených časech (x) systém náležitě upozorňuje na zjištěné případy přítomnosti škodlivého kódu.
  11. **Vzájemné oddělení testovacích a produkčních systémů**: Zhotovitel zajistí, aby (i) testovací a produkční systémy byly alespoň logicky odděleny s cílem snížit riziko neoprávněného přístupu nebo neoprávněné změny produkčních systémů. (ii) V případě, že vzájemné oddělení není možné, Zhotovitel zajistí zavedení speciálně upravených postupů pro proces řízení změn a proces řešení incidentů a mimořádných situací, které umožní rychle a přiměřeně reagovat na narušení produkčních systémů a problémy v těchto systémech. (iii) V testovacích nebo vývojových prostředích nesmí být produkční data povolena a musí být anonymizována vždy, obsahují-li osobní údaje nebo osobně identifikovatelné informace (PII).
  12. **Vývoj/pořizování softwaru**: Zhotovitel zajistí, aby interně vyvinutý software nebo software získaný z externích zdrojů, který se používá ke zpracování, ukládání nebo předávání informací společnosti E.ON, nevykazoval žádné bezpečnostní chyby z hlediska kritérií „OWASP TOP Ten“ a „SANS Top 25 Most Dangerous Software Errors“.
  13. **Prověřování bezpečnostních zranitelností**: Zhotovitel zajistí, aby (i) veřejně přístupné systémy byly pravidelně (nejméně jednou ročně) testovány na zranitelnosti a chyby v nastavení provedením dynamických testů (penetrační test nebo prověřování zranitelností), (ii) společnost E.ON byla bez zbytečného odkladu informována o veškerých zjištěních z těchto testů, která jsou pro společnost E.ON relevantní; (iii) kritické zranitelnosti byly společnosti E.ON okamžitě oznámeny. (iv) Zhotovitel poskytne pomoc a podporu při kontrolách procesu správy bezpečnostních zranitelností a oprav (tzv. „záplat“) prováděné pro společnost E.ON. (v) Ošetření bezpečnostních zranitelností se řeší na základě úrovní rizika těchto zranitelností a dle příslušných časových harmonogramů smluvních stran.
  14. **Úroveň aktuálnosti bezpečnostních záplat (tzv. patchů)**: Zhotovitel zajistí odstranění zranitelností realizací procesu správy bezpečnostních záplat, v jehož rámci (i) identifikuje a získá bezpečnostní záplaty z autorizovaných zdrojů, jakmile jsou k dispozici, (ii) rozhodne, kdy je třeba bezpečnostní záplaty nasadit, (iii) otestuje bezpečnostní záplaty na základě známých kritérií, (iv) nasadí bezpečnostní záplaty v dohodnutém časovém rámci, (v) eviduje stav implementace bezpečnostních záplat (např. v konfigurační databázi CMDB). (vi) Zhotovitel je oprávněn bezpečnostní záplaty používat v prostředí IT, včetně virtualizačních hypervisorů, virtuálních počítačů, operačních systémů a aplikací, pokud to nepříznivě neovlivní zachování důvěrnosti, integrity nebo dostupnosti informací společnosti E.ON.
  15. **Minimální požadavky na přihlašovací údaje:** Zhotovitel zajistí splnění minimálních požadavků společnosti E.ON na přihlašovací údaje (doporučená je dvoufaktorová autentizace) prostřednictví E.ON Single-Sign-On federativních služeb. Musí být uplatňovány tyto zásady: princip minimálních oprávnění, udělení těchto oprávnění výhradně osobám, které je potřebují ke své činnosti (‚need-to-know princip“) a jasné oddělení zodpovědnosti („segregation of duties“). Dále je třeba uplatňovat koncepci řízení přístupu na základě rolí.
  16. **Požadavky na návrh sítí:** U aplikací, které jsou přístupné prostřednictvím internetu, musí být jak vícevrstvá architektura, tak služby umístěné v demilitarizované zóně (DMZ). Síťové segmenty musí být vhodnými bezpečnostními opatřeními odděleny od segmentů s nízkou a střední úrovní ochrany s cílem zabránit přenosu dat mezi segmenty. Síťové segmenty s velmi vysokou úrovní ochrany by měly být pokud možno také odděleny od segmentů s vysokou úrovní ochrany a vůči těmto segmentům zabezpečeny.
  17. **Standardy bezpečnostního nastavení (tzv. „hardening“)**: Všechny informačních a síťové systémy musí být standardně bezpečně nastaveny a řádně zabezpečeny. To zahrnuje: (i) zakázání a blokování nepotřebných aplikací, služeb, nástrojů, protokolů a rozhraní, (ii) vymazání nebo přinejmenším změna výchozích uživatelských jmen a hesel od výrobce, (iii) aktivace bezpečnostních nástrojů a konfigurací ke zvyšování zabezpečení a (iv) zabránění přenosu technických informací externím subjektům.
  18. **Protokolování bezpečnostních událostí**: V zájmu zjištění a vyšetřování neoprávněného přístupu k informacím společnosti E.ON a neoprávněné manipulace s nimi zajistí, aby (i) u všech systémů provozovaných Zhotovitelem za účelem vytváření, ukládání, zpracování a předávání informací společnosti E.ON bylo vždy povoleno protokolování událostí (logování), (ii) tyto systémy byly nakonfigurovány tak, aby generovaly bezpečnostní události (včetně událostí, jako jsou úspěšné a neúspěšné pokusy o přihlášení uživatele, vytvoření / úprava / odstranění služby, vytvoření / úprava / odstranění objekt, havárie systému, odstranění uživatelských účtů) a atributy událostí související s každou konkrétní událostí (např. datum, čas, ID uživatele, název souboru a IP adresa), (iii) konzistentní, důvěryhodné datové a časové zdroje byly zárukou, že protokoly událostí používají přesná časová razítka (např. pomocí serverů NTP), (iv) protokoly bezpečnostních událostí byly chráněny před neoprávněným přístupem a náhodnou nebo úmyslnou úpravou / přepsáním
  19. **Dodržování předpisů (compliance)**: Zhotovitel zajistí, aby (i) všechny systémy, které vytvářejí, ukládají, zpracovávají nebo předávají informace společnosti E.ON, byly pravidelně kontrolovány z hlediska dodržování vlastních „bezpečnostních politik/standardů“ Zhotovitele. (ii) Vlastní „bezpečnostní politiky/standardy“ Zhotovitele musí být v souladu s požadavky s certifikáty uvedenými v oddílech 2 a 3 této přílohy. (iii) Zhotovitel společnosti E.ON na vyžádání předloží prohlášení o technické shodě za účelem prokázání, že tyto technické kontroly shody proběhly pro každý prostředek (aktivum) v rámci prostředí IT. Prohlášení o shodě musí obsahovat přiřazení mezi souvisejícími kontrolami vyplývajícími z oddílů 2 a 3 této přílohy a kontrolou technické shody. (iv) Zhotovitel vlastní „bezpečnostní zásady / standardy“ zpřístupní před Datem účinnosti a poté na vyžádání společnosti E.ON.
  20. **Bezpečná likvidace a opětovné použití**: Zhotovitel zajistí, aby hardware, který má být vyřazen z provozu, (i) byl před jeho opětovným použitím, prodejem nebo vrácením vyčištěn tak, aby všechny informace společnosti E.ON byly v celém rozsahu bezpečně smazány (ii) nebo bezpečně zničeny. (iii) Smazání nebo zničení je třeba provést bezpečným způsobem pomocí nejmodernějších technologií a postupů, jako jsou nástroje a postupy definované v NIST SP 800-88 Guideline for Media Sanitization (Postupy pro odstraňování dat z médií). (iv) Zhotovitel na vyžádání společnosti E.ON předloží koncepci bezpečného odstraňování a smazání, jakož i důkazy o provedeném bezpečném odstranění a vymazání informací společnosti E.ON.
  21. **Bezpečnost lidských zdrojů:** Za každou osobu, která jedná jménem Zhotovitele a byla jí udělena přístupová oprávnění (místně nebo vzdáleně), musí být společnosti E.ON poskytnuty osobní identifikační údaje. Zhotovitel zajistí ověření totožnosti fyzických osob a dále zajistí, aby nikdo nezneužil přístupu nebo oprávnění udělených Zhotovitelem. Zhotovitel dále přejímá odpovědnost za případné škody způsobené neoprávněným přístupem a/nebo použitím informací společnosti E.ON. Zhotovitel pověří plněním zadaných úkolů výhradně pracovníky, kteří jsou k jejich plnění prokazatelně odborně způsobilí.
  22. **Bezpečnost v oblasti dodavatelského řetězce**: Zhotovitel zajistí identifikaci a řízení rizika bezpečnosti informací v každé fázi vztahů s externími zhotoviteli hardwaru a softwaru v celém dodavatelském řetězci tím, že (i) začlení požadavky na bezpečnost informací do formálních smluv a ii) ověří plnění těchto požadavků. (iii) Zhotovitel zajistí, aby subdodavatelé, kteří se podílejí na zpracování, ukládání, předávání nebo likvidaci informací společnosti E.ON, splňovali minimálně požadavky dohodnuté v této příloze. (iv) Zhotovitel je zodpovědný za zajištění náležitého řízení Subdodavatele(ů) a za dodržování opatření prováděných externě.

1. **Požadavky na ochranu osobních údajů** 
   1. Kontrola přenosu
      1. Požadavky na pracovníky v oblasti mlčenlivosti
         1. Všichni pracovníci, kteří zpracovávají osobní údaje pomocí automatizovaných procesů, musí dodržovat pravidla mlčenlivosti.
         2. Noví pracovníci musí být informováni o ochraně údajů pro potřeby nakládání s osobními údaji.
         3. Všechny zúčastněné strany si jsou vědomy otázek souvisejících s bezpečností a ochranou údajů.
         4. Osoby, které osobní údaje zpracovávají, jsou prokazatelně poučeni o bezpečném nakládání s osobními údaji na pracovišti.
         5. Jsou definována jasná pravidla pro postup v případě odchodu a propouštění pracovníků.
      2. Anonymizace / pseudonymizace
         1. Pro potřeby přenosu osobních údajů jsou využívány techniky anonymizace a pseudonymizace – pokud je to možné.
         2. V případě pseudonymizace údajů je nutné zajistit, aby pseudonym nebyl příjemci zasílán společně se skutečným jménem.
   2. Kontrola vstupů – Protokoly

(i) Pověřenec pro ochranu osobních údajů sleduje namátkově dodržování pokynů / zásad pro protokolování přístupů.

* 1. Kontrola objednávek
     1. Pověřenec pro ochranu osobních údajů (dle článků 37 až 39 obecného nařízení o ochraně osobních údajů (GDPR) a vnitrostátních právních předpisů)
        1. Je jmenován pověřenec pro ochranu osobních údajů, pokud je k tomu dodavatel povinen dle čl. 37 GDPR.
        2. U pověřenců pro ochranu osobních údajů nesmí docházet ke střetu zájmů.
        3. Pověřenec pro ochranu osobních údajů musí mít příslušnou kvalifikaci a musí být spolehlivý dle požadavků konkrétní společnosti.
        4. Pověřenec pro ochranu osobních údajů je jmenován písemnou formou.
        5. Vedení společnosti musí pověřence pro ochranu osobních údajů v jeho práci podporovat.
        6. Pověřenec pro ochranu osobních údajů je přímo podřízen vedení společnosti a přímo se mu zodpovídá.
        7. Pověřenec pro ochranu osobních údajů je včas informován o nových procesech či o modifikaci stávajících procesů a přímo se podílí na jejich plánování.
        8. Pověřenec pro ochranu osobních údajů aktivně přispívá k navrhování procesů.
  2. Smluvní požadavky
     1. Všichni subdodavatelé zapojení do zpracování objednávky jsou smluvně vázáni vůči Zhotoviteli.
     2. Smluvní dohoda mezi Zhotovitelem a subdodavatelem musí splňovat podmínky uvedené v článku 28, odstavci 3 GDPR.
  3. Výběr subdodavatelů
     1. Zhotovitel zdokumentuje rozhodnutí o subdodavateli a důvody pro jeho výběr.

**2.6** Další pravidla řízení ochrany osobních údajů

* + 1. Je zaveden systém ochrany osobních údajů a řízení rizik v souladu s požadavky GDPR. Externě zajišťované služby infrastruktury IT jsou do systému řízení rizik plně integrovány.
    2. V souvislosti se zpracováním osobních údajů probíhá analýza rizik dle předem stanovených transparentních kritérií a zjištěná rizika v bezpečnosti informací a ochrany osobních údajů jsou na základě těchto kritérií hodnocena a řádně řešena pomocí závazného a kontinuálního procesu. Účinnost přijatých opatření je hodnocena pravidelnými interními audity.
    3. Jsou vydávány pravidelné zprávy o ochraně osobních údajů popisující aktuální stav a účinnost systému řízení ochrany osobních údajů, včetně všech případných selhání či relevantních případů narušení ochrany osobních údajů/ bezpečnosti. Tyto zprávy jsou Zhotovitelem poskytnuty na vyžádání.
    4. Všechny dokumenty, které by měly být dostupné jsou vydávány v takové formě, aby mohly být poskytnuty třetí straně k posouzení zavedených opatření k ochraně osobních údajů a informací. Veškerá dokumentace je dle potřeby aktualizována. Dokumentace s upraveným obsahem je dostupná na vyžádání.
    5. Vedení společnosti Zhotovitele je plně informováno a zapojeno do informační bezpečnosti a ochrany osobních údajů formou příslušných komunikačních, eskalačních a rozhodovacích procesů. Vedení společnosti Zhotovitele zajistit, že činnosti a zodpovědnosti mohou být vykonávány v souladu s požadavky a v uspokojivé kvalitě.
    6. Jsou prokazatelně vyčleněny dostatečné zdroje na zřízení, implementaci, provozování, monitoring, hodnocení, údržbu a zlepšování systému řízení ochrany osobních údajů, stejně tak jako dostupného prokazování jeho existence.
    7. Do provozu systému řízení ochrany osobních údajů se mohou zapojit pouze zaměstnanci s dostatečnou kvalifikací a znalostmi nutnými pro realizaci příslušných úkolů. Tato kvalifikace a znalosti jsou zajišťovány formou pokynů a školení.
    8. Pravidelně, a alespoň jednou ročně, a nezávisle na hodnocení bezpečnosti IT a rizik probíhá interní audit stavu ochrany osobních údajů. Smyslem auditu je zjišťovat odchylky skutečného stavu ochrany údajů od smluvně garantované úrovně ochrany osobních údajů (tzn. všech dohodnutých technických a organizačních opatření). Tato zjištění pak dle potřeby slouží pro hodnocení rizika a lze je na vyžádání předložit.
    9. Výstupem auditu řízení ochrany osobních údajů je akční plán, který jasně definuje, jaké kroky je nutné přijmout a v jakém časovém horizontu tak, aby byly zjištěné problémy odstraněny.

Do plánu lze na vyžádání nahlédnout.

* + 1. Systém řízení ochrany osobních údajů je neustále zlepšován pomocí přístupu založeném na PDCA (naplánuj-proveď-ověřjednej), v jehož rámci je Společnost E.ON na vyžádání informována o fázi plánování a účastní se fáze realizace (Act – jednej), pokud se vyhrazené zdroje a zdroje pro více klientů týkají osobních údajů Společnosti E.ON.
    2. Účinnost systému řízení ochrany osobních údajů je ověřována interními a externími testy (audity).
    3. Jsou jmenovány příslušné kontaktní osoby a jsou poskytnuty konkrétní kontaktní informace a stanoveny postupy pro výměnu informací se Společností E.ON a koordinaci opatření k ochraně osobních údajů.

**2.7** Kontroly dostupnosti – Ukládání firemních dokumentů

**2.7.1** Dokumenty a elektronicky uložená data jsou po uplynutí zákonné, povinné nebo smluvní archivační doby skartovány a elektronicky uložená data vymazána dle plánu výmazu v souladu s příslušnými právními předpisy na ochranu osobních údajů.

1. **Normy** 
   1. Zhotovitel souhlasí s tím, že služby budou dodávány v souladu s těmito normami:
      1. ISO/IEC 27001: Všechna zařízení pro hostování dat a podpůrné služby, jakož i procesy, v jejichž rámci jsou ukládány nebo zpracovávány informace společnosti E.ON, musí být provozovány v souladu s normou ISO / IEC 27001 „Informační technologie – bezpečnostní techniky – systémy managementu bezpečnosti informací – požadavky“.
      2. Zhotovitel se zavazuje, že na vyžádání společnosti E.ON předloží příslušná prohlášení o shodě.
2. **Kontaktní osoby a výměna informací** 
   1. Obě Smluvní strany souhlasí se oznámením a poskytnutím kontaktních osob pro následující procesy bezpečnosti IT:
      1. Řízení shody s požadavky: průběžná výměna informací o dodržování požadavků, průběžné předkládání zpráv uvedených v této příloze a projednání a odsouhlasení opatření k řešení stávajících případů neshod s požadavky a souvisejících rizik.
      2. Řízení bezpečnostních incidentů: výměna informací o bezpečnostních incidentech nebo událostech, které by mohly vést k incidentu, který by ovlivnil nebo mohl ovlivnit prostředí IT provozované k ukládání nebo zpracování informací společnosti E.ON. „Řízení bezpečnostních incidentů“ zahrnuje také správu žádostí společnosti E.ON o forenzní analýzu.
      3. Řízení rizik: průběžná výměna informací o činnostech řízení rizik prováděných Zhotovitelem s cílem zajistit, aby rizika v oblasti bezpečnosti informací byla průběžně identifikována, hodnocena, ošetřována, monitorována a udržována v přijatelných mezích.
      4. Řízení zranitelností: výměna informací o zranitelnostech, které ovlivňují nebo by mohly ovlivnit prostředí IT provozované k ukládání nebo zpracování informací společnosti E.ON, a projednání a odsouhlasení opatření k odstranění / zmírnění stávajících zranitelností.
      5. Správa bezpečnostních záplat: výměna informací o dohodnutých časových obdobích údržby a instalace bezpečnostních záplat (tzv. „patchů“).
      6. Správa identit a přístupu: výměna informací o tématech souvisejících se správou identit a přístupu.
      7. Ochrana údajů: výměna informací o činnostech a incidentech souvisejících s ochranou osobních údajů.
   2. Obě Smluvní strany souhlasí s tím, že budou v rámci výše uvedených bezpečnostních procesů spolupracovat a vyměňovat si informace. Smluvní strany se dohodnou na technických prostředcích pro výměnu informací a klíčových ukazatelů výkonnosti (Key Performance Indicators, KPI) s cílem zajištění shody s dohodnutými bezpečnostními postupy.
   3. Obě Smluvní strany souhlasí s tím, že byly jmenovány kontaktní osoby pro výše uvedené bezpečnostní postupy a že může být provedena jejich personální výměna. V případě personální výměny kontaktní osoby Smluvní strana, která výměnu jmenované kontaktní osoby provede, o této skutečnosti bezodkladně uvědomí druhou Smluvní stranu.

*Kontaktní osoba společnosti E.ON*

Ochrana osobních údajů

Jméno a příjmení: Jindřich Veselý

Telefon: (+420) 733 670 559

E-mailová adresa: jindrich.vesely@eon.cz

Bezpečnost informací

Jméno a příjmení: Josef Ječmen

Telefon: (+420) 724 606 913

E-mailová adresa: josef.jecmen@eon.com

*Kontaktní osoba Zhotovitele*

Jméno a příjmení: doplní dodavatel

Telefon: doplní dodavatel

E-mailová adresa: doplní dodavatel