PLZEŇSKÁ TEPLÁRENSKÁ

Více než energie

Kupní smlouva

číslo smlouvy kupujícího: D2026/0113

(dále také jako „smlouva“ nebo „kupní smlouva“)

Obnova bezpečnostních bran (firewally)

Plzeňská teplárenská, a. s., Doubravecká 2760/1, 301 00 Plzeň
[redacted]
e-mail: [redacted] www.plzenskateplarenska.cz
IČ: 49790480, DIČ: CZ49790480
bankovní spojení: [redacted]
Společnost zapsána v Obchodním rejstříku u Krajského soudu v Plzni, oddíl B, vložka 392

Město Plzeň

CERTIFIED
ISO 9001 - ISO 14001
ISO 50001

[redacted]

kterou níže uvedeného dne, měsíce a roku uzavřely ve smyslu ustanovení § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění, tyto smluvní strany

1. jako prodávající

[redacted]

(dále jen „prodávající")

a

2. jako kupující

Plzeňská teplárenská, a.s.
sídlem 301 00 Plzeň, Doubravecká 2760/1
zapsaná v OR vedeném KS v Plzni, oddíl B, vložka 392
IČ: 497 90 480
DIČ: CZ49790480
bankovní spojení: [redacted]
č. účtu:
zastoupená: [redacted]

(dále jen „kupující")

takto:

Článek I.
Předmět smlouvy

(1) Prodávající se zavazuje dodat kupujícímu zboží:

Firewally,

a to včetně potřebných licencí a provedení implementace celého řešení

dle specifikace uvedené v Technickém zadání a jeho přílohách, které jako **příloha č. 1** tvoří nedílnou součást této kupní smlouvy, a dále převést na kupujícího vlastnické právo k tomuto zboží (dále jen „zboží").

(2) Prodávající se zavazuje dodat se zbožím doklad o zakoupeném supportu a dále se zavazuje nainstalovat a nakonfigurovat firewally certifikovaným odborníkem od výrobce, jak je uvedeno v Technickém zadání, které je **přílohou č. 1** této smlouvy. Prodávající se dále zavazuje na každou část implementace předat kupujícímu příslušné akceptační protokoly.

(3) Kupující se zavazuje zaplatit prodávajícímu za zboží kupní cenu stanovenou v článku II., odst. (1) této smlouvy.

[redacted]

Článek II.
Kupní cena a platební podmínky

(1) Účastníci se dohodli, že kupní cena za zboží činí celkem: [redacted] **Kč.**

Uvedená cena je úplná a konečná, je včetně dopravy do sídla kupujícího, je bez daně z přidané hodnoty a není stanovena na základě odhadu.

(2) Shora uvedená cena bude zaplacena následujícím způsobem:

a) po dodání HW a licencí vystaví zhotovitel do 15 dnů dílčí fakturu na částku ve výši [redacted]% z celkové ceny díla dle odstavce (1) navýšené o případnou DPH dle platných právních předpisů. Přílohou faktury bude kopie dílčího předávacího protokolu o dodání HW a licencí, který bude podepsán oběma smluvními stranami;

b) neprodleně po provedení implementace celého řešení, tj. po předání akceptačních protokolů a podpisu Protokolu o předání a převzetí provedené implementace celého řešení, vystaví zhotovitel konečnou fakturu (daňový doklad) na částku ve výši [redacted]% z celkové ceny díla dle odstavce (1) navýšené o případnou DPH dle platných právních předpisů. Přílohou faktury bude kopie akceptačních protokolů a Protokolu o předání a převzetí provedené implementace celého řešení, který bude podepsán oběma smluvními stranami.

Fakturu zhotovitel vždy odešle neprodleně po jejím vystavení objednateli. Zhotovitel je oprávněn fakturovat objednateli v tištěné nebo elektronické podobě. V případě elektronické fakturace odešle fakturu na e-mailovou adresu [redacted]. Lhůta splatnosti faktury je 30 dnů od jejího vystavení. Faktura bude hrazena formou bankovního převodu. Ocitne-li se objednatel v prodlení se zaplacením ceny, má zhotovitel právo požadovat úrok z prodlení ve výši [redacted]% z dlužné částky za každý den prodlení.

(3) Faktury dle článku II., odst. (2) této smlouvy musí kromě náležitostí požadovaných obecně závaznými právními předpisy a touto smlouvou, obsahovat také:

a) označení peněžního ústavu a číslo účtu prodávajícího,
b) číslo kupní smlouvy a číslo objednávky,
c) údaj o době splatnosti faktury uvedený v souladu s touto smlouvou,
d) kopie příslušného předávacího protokolu,
e) rozpis materiálu včetně rozpisu konečných cen (může být i na samostatné příloze).

V případě, že faktura nebude obsahovat náležitosti stanovené obecně závaznými právními předpisy a/nebo náležitosti stanovené v této smlouvě, není kupující povinen plnit podle této faktury. Kupující v takovém případě vrátí bez zbytečného odkladu takto vadně vystavenou fakturu prodávajícímu s uvedením důvodu jejího vrácení. Prodávající je povinen dle povahy závad vystavit kupujícímu opravenou nebo nově vyhotovenou fakturu. Nová lhůta splatnosti (opět v délce 30 dnů) pak počíná běžet ode dne vystavení opravené nebo nově vyhotovené faktury, kupujícímu neprodleně odeslané.

(4) Prodávající je povinen řídit se pro účely uplatňování DPH klasifikací CZ-CPA v souladu s § 92e) zákona č. 235/2004 Sb., o dani z přidané hodnoty v platném znění (dále také jako „zákon o DPH"), a příslušnými pokyny ministerstva financí.

(5) Kupující je oprávněn provést v souladu s §109a zákona o DPH zajišťovací úhradu DPH na účet příslušného finančního úřadu, jestliže se prodávající stane ke dni uskutečnění zdanitelného plnění nespolehlivým plátcem.

(6) Prodávající jako plátce DPH prohlašuje, že splnil svou povinnost stanovenou mu zákonem o DPH k oznámení čísel svých bankovních účtů používaných pro ekonomickou činnost svému správci

[redacted]

daně a zavazuje se na fakturách - daňových dokladech, které budou vystavovány za jím poskytnutá plnění dle této smlouvy uvádět pro platby vždy výhradně ta čísla účtů, která byla oznámena příslušnému správci daně a jím zveřejněna v databázi umožňující dálkový přístup.

(7) V případě, že prodávající (i) pro platbu nebo její část na příslušné faktuře - daňovém dokladu uvede účet, který není shodný s jeho účtem aktuálně zveřejněným jeho správcem daně způsobem, který umožňuje dálkový přístup, a/nebo (ii) bude zveřejněn jako nespolehlivý plátce, a to způsobem předpokládaným zákonem o DPH, a/nebo (iii) má účet, na který má být poskytnuta zčásti nebo zcela bezhotovostním převodem platba za jím zdanitelné plnění uskutečněné v tuzemsku, vedený poskytovatelem platebních služeb mimo tuzemsko, má kupující právo volby mezi (a) vrácením příslušné faktury k opravě nebo (b) zadržením DPH z každé fakturované platby za poskytnuté zdanitelné plnění a jejím uhrazením (aniž k tomu bude vyzván) za prodávajícího příslušnému správci daně. Pokud bude postupováno dle písm. (b) výše platí, že po provedení úhrady DPH příslušnému správci daně je úhrada zdanitelného plnění prodávajícímu bez příslušné DPH (tj. pouze základu daně) smluvními stranami považována za řádnou úhradu dle této smlouvy (tj. základu daně i výše DPH), a tomu nevzniká žádný nárok na úhradu případných úroků z prodlení, penále, náhrady škody nebo jakýchkoli dalších sankcí vůči kupujícímu, a to ani v případě, že by mu podobné sankce byly vyměřeny správcem daně.

(8) Pokud kdykoliv po dobu trvání této smlouvy vyjde najevo, že prodávající neoznámil svému správci daně čísla bankovních účtů používaných pro ekonomickou činnost anebo že ve fakturaci uvádí jiná, než oznámená a správcem daně zveřejněná čísla účtů, je kupující oprávněn postupovat způsobem dle článku II., odst. (7) této smlouvy; kupující je v takovém případě rovněž oprávněn od této smlouvy odstoupit.

Článek III.
Dodání zboží

(1) Prodávající je povinen dodat zboží nejpozději **do 30. 6. 2026.**

(2) Prodávající je povinen v místech určených kupujícím provést všechny související činnosti specifikované v **příloze č. 1**. Smluvní strany se dohodly, že související činnosti budou provedeny nejpozději **do 31. 8. 2026.**

Místa implementace určená kupujícím se nacházejí v provozovnách kupujícího:

a) Areál TEPLÁRNA, Doubravecká 2760/1, Plzeň,
b) Areál ENERGETIKA, Tylova 1/57, Plzeň,
c) ZEVO Plzeň, Chotíkov 492, Chotíkov,
d) Vodárna Radčice, V Radčicích 331, Plzeň – Radčice
e) Objekt VS-7L Komenského 99, Komenského 1329/99, Plzeň.

(3) Dopravu zboží zajistí prodávající na vlastní náklady a nebezpečí do sídla kupujícího, a to konkrétně do Plzeňské teplárenské, a.s., areál TEPLÁRNA, Doubravecká 2760/1, 301 00 Plzeň, kontaktní osoba: Ing. Ondřej Červený, tel.: mob.: 605 913 104.

(4) Prodávající je povinen dodat zboží ve lhůtě stanovené v článku III., odst. (1) této smlouvy a na vnější viditelné části obalu uvést svoji adresu a číslo objednávky.

(5) Kupující je oprávněn odmítnout převzít zboží, jestliže dodané zboží není označeno na obalu v souladu s článkem III., odst. (3) této smlouvy a dále, má-li zjevné vady nebo jestliže obal zboží je tak vážně poškozen, že kupující může mít důvodně za to, že je zboží poškozeno.

[redacted]

(6) Prodávající je povinen zboží specifikované v článku I. této smlouvy a v její **příloze č. 1** dodat v provedení v nich uvedené. Není-li provedení dané, pak v takovém, které je obvyklé pro jeho běžný účel.

(7) Prodávající je povinen zabalit zboží pro přepravu tak, aby bylo řádně uchováno a chráněno před vnějšími vlivy a zásahy třetích osob, které lze při přepravě obvykle předpokládat.

(8) Smluvní strany sjednaly, že zboží se považuje za dodané okamžikem potvrzení dodacího listu ze strany kupujícího. V rámci potvrzení dodacího listu bude uvedeno, zda byl porušen obal zboží či jiné zjevné vady, které jsou seznatelné při zběžném pohledu.

(9) Vlastnictví zboží na kupujícího přechází okamžikem potvrzení dodacího listu.

(10) Nebezpečí škody na zboží přechází na kupujícího s přechodem vlastnictví.

Článek IV.
Záruka za jakost

(1) Prodávající přebírá závazek, že zboží si zachová nezávadnost po dobu **36 měsíců** (záruční doba) od převzetí zboží a umožní tak kupujícímu jeho řádné užívání.

(2) Kupující může oznámit prodávajícímu vady kdykoliv během záruční doby.

(3) Odpovědnost prodávajícího za vady, na něž se vztahuje záruka za jakost, nevznikne, jestliže tyto vady byly způsobeny po přechodu nebezpečí škody na zboží vnějšími událostmi a nezpůsobil je prodávající.

(4) Záruční doba neběží po dobu, po kterou kupující nemůže zboží užívat pro jeho vady, za něž odpovídá prodávající.

Článek V.
Nároky z vad zboží

(1) Zboží má vady, jestliže neodpovídá kvalitativním podmínkám, rozsahu, vlastnostem a kritériím stanoveným touto smlouvou a/nebo obecně závaznými právními předpisy a/nebo ČSN. Za vady zboží se považují rovněž vady veškerých a úplných dokladů a podkladů vztahujících se ke zboží, které je prodávající povinen kupujícímu na základě této smlouvy spolu se zbožím dodat. V případě, že budou dodané doklady vykazovat vady, je kupující oprávněn tyto vrátit prodávajícímu na jeho náklady a/nebo prodávajícího vyzvat k dodání dokladů bez vad. Prodávající je v takovém případě povinen bez zbytečného odkladu, nejpozději však do 3 dnů od vrácení vadných dokladů nebo od doručení výzvy kupujícího, dodat kupujícímu úplné doklady bez vad.

(2) Má-li dodané zboží vady, může kupující v záruční době:

a) požadovat odstranění vady formou dodání náhradního zboží za zboží vadné, dodáním chybějícího zboží nebo požadovat odstranění právních vad, a to ve lhůtě stanovené kupujícím,

b) požadovat odstranění vad opravou zboží, jestliže vady jsou opravitelné, a to ve lhůtě stanovené kupujícím,

c) požadovat přiměřenou slevu z kupní ceny,

d) odstoupit od této smlouvy,

[redacted]

e) sám nebo prostřednictvím třetí osoby zboží zkontrolovat, nechat odstranit příslušnou vadu anebo zajistit provedení opravy zboží anebo jeho části anebo zajistit dodání chybějícího zboží místo prodávajícího, přičemž prodávající v takovém případě nahradí kupujícímu veškeré náklady s tím spojené, a to bezodkladně na výzvu kupujícího, aniž by tímto bylo jakkoliv dotčeno právo kupujícího na náhradu škody v plné výši.

(3) Kupující může zvolit podle vlastního uvážení mezi nároky uvedenými v článku V., odst. (1) této smlouvy. Uplatněný nárok může kupující měnit i bez souhlasu prodávajícího. Nároky z vad zboží se nedotýkají nároku na náhradu škody nebo na smluvní pokutu.

Článek VI.
Smluvní pokuty

(1) Dostane-li se prodávající do prodlení s dodáním zboží, má kupující nárok na smluvní pokutu ve výši [redacted] % z celkové ceny zboží za každý den prodlení.

(2) Dostane-li se prodávající do prodlení s provedením všech souvisejících činností, má kupující nárok na smluvní pokutu ve výši [redacted] % z celkové ceny zboží za každý den prodlení.

(3) V případě porušení povinností uvedených v článku VIII. Kybernetická bezpečnost této smlouvy a souvisejících bezpečnostních politik objednatele je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši [redacted] Kč za každý takový případ.

(4) Pro každý případ porušení povinnosti ochrany informací (dle článku VII. této smlouvy) se stanovuje smluvní pokuta ve výši [redacted] Kč pro informace klasifikace „interní", [redacted] Kč pro informace klasifikace „důvěrné" a [redacted] Kč pro informace klasifikace „tajné", za každý takový případ.

(5) Dostane-li se prodávající do prodlení s odstraněním vady zboží, má kupující nárok na smluvní pokutu ve výši [redacted] % z celkové ceny zboží za každý den prodlení.

(6) Smluvní pokuta bude kupujícím fakturována prodávajícímu vždy bez zbytečného odkladu. Lhůta splatnosti smluvní pokuty činí 30 dnů od vystavení faktury kupujícím.

(7) Ujednání o smluvní pokutě se nedotýká práva kupujícího požadovat náhradu škody způsobenou přerušením povinnosti, na kterou se vztahuje smluvní pokuta. Kupující je také oprávněn domáhat se náhrady škody přesahující smluvní pokutu.

Článek VII.
Ochrana informací

(1) Prodávající má zavedenou kategorizaci důvěrnosti informací pro zajištění přiměřenosti ochrany informačních aktiv/informací. Jedná se o kategorie, které slouží k rozlišení míry ochrany informací, které do nich spadají, přičemž objednatel rozlišuje 4 stupně informací, a to „veřejné", „interní", „důvěrné" a „tajné". Charakteristika jednotlivých kategorií včetně pravidel ohledně zacházení s příslušnými informacemi je uvedena v přílohách PIKYB. Prodávající se zavazuje nakládat s daty s ohledem na klasifikaci definovanou kupujícím.

(2) Veškeré informace, které prodávající vědomě či nevědomě od kupujícího obdrží, jsou považovány dle klasifikace kupujícího za „interní", pokud nebudou předávané informace jednoznačně označeny jinou klasifikací.

[redacted]

(3) Prodávající se zavazuje, že nezpřístupní (vyjma informací veřejných) třetí osobě informace (bez ohledu na formu jejich zachycení), které získal během jednání vedoucích k uzavření této smlouvy nebo během plnění závazků z této smlouvy.

(4) Za třetí osoby dle odst. (3) tohoto článku se nepovažují:

- zaměstnanci smluvních stran a osoby v obdobném postavení,
- orgány smluvních stran a jejich členové,
- ve vztahu k informacím kupujícího poddodavatelé prodávajícího,
- ve vztahu k informacím prodávajícího externí dodavatelé kupujícího, a to i potenciální,
- osoby vázané na základě zvláštního právního předpisu povinností mlčenlivosti za předpokladu, že se podílejí na plnění této smlouvy nebo plnění spojeném s plněním dle této smlouvy, informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění informací je v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny smluvním stranám v této smlouvě.

(5) Prodávající se zavazuje přijmout technická a organizační opatření nezbytná k ochraně dostupnosti, důvěrnosti a integrity informací a v plném rozsahu zachovávat povinnost mlčenlivosti vyplývající z této smlouvy, aby nemohlo dojít k nežádoucímu zpřístupnění informací jiné osobě a případně k jejich zneužití. Prodávající je povinen neprodleně informovat kupujícího o všech kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy a o způsobu řízení rizik na své straně včetně zbytkových rizik souvisejících s plněním smlouvy.

(6) Prodávající se zavazuje poučit a zavázat mlčenlivostí veškeré osoby vč. všech poddodavatelů, které se na jejich straně budou podílet na plnění této smlouvy, o výše uvedených povinnostech ochrany informací a dále se zavazují vhodným způsobem zajistit dodržování těchto povinností všemi osobami podílejícími se na plnění této smlouvy. Prodávající je povinen předem informovat objednatele o všech fyzických osobách přicházejících do kontaktu s důvěrnými informacemi kupujícího, zejména o osobách zastávajících bezpečnostní role, penetračních testerech či administrátorech.

(7) Pokud při poskytování předmětu plnění dochází ke zpracování osobních údajů, zavazují se obě smluvní strany zajistit uzavření samostatných smluv (tj. smluv se svými poddodavateli, zaměstnanci a případnými dalšími osobami podílejícími se na poskytování plnění z této smlouvy) ve smyslu příslušných ustanovení Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

(8) Kupující jako správce zpracovává osobní údaje prodávajícího, resp. jeho zástupců případně kontaktních osob či dalších osob, poskytnuté v rámci smlouvy výhradně pro účely související s plněním této smlouvy. Všechny informace týkající se zpracování osobních údajů, včetně práv subjektů s tímto zpracováním souvisejících, jsou k dispozici v aktuální verzi na webových stránkách objednatele www.plzenskateplarenska.cz v sekci „O nás - Zpracování osobních údajů".

(9) Prodávající bere na vědomí, že veškeré aktivity prodávajícího a jeho plnění realizované v prostředí kupujícího jsou monitorovány a vyhodnocovány z hlediska zajištění kybernetické bezpečnosti a bezpečnosti informací.

(10) Za porušení povinnosti mlčenlivosti třetími osobami, které se budou podílet na plnění předmětu smlouvy, odpovídá prodávající, jako by povinnost porušil sám.

(11) Ukončení účinnosti této smlouvy z jakéhokoliv důvodu se nedotkne ustanovení tohoto článku a jeho účinnost přetrvá i po ukončení účinnosti této smlouvy.

[redacted]

Článek VIII.
Kybernetická bezpečnost

(1) Není-li v této smlouvě nebo v souladu s touto smlouvou stanoveno jinak, prodávající tímto bere na vědomí, že:

a) kupující je poskytovatelem služby v oblasti energetiky ve smyslu § 3 zákona č. 264/2025 Sb., o kybernetické bezpečnosti ve znění pozdějších předpisů (dále jen „ZoKB“);

b) je z pohledu kupujícího významným dodavatelem ve smyslu § 2 písm. i) vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností či dodavatelem do stanoveného rozsahu ve smyslu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (dále jen souhrnně jako „VoKB“);

c) prodávající se zavazuje dodržovat veškeré povinnosti vyplývající z této skutečnosti, zejména pak povinnosti stanovené v ZoKB, VoKB a souvisejících právních předpisech.

(2) Prodávající umožní kupujícímu kdykoli po dobu platnosti této smlouvy provedení zákaznického auditu:

a) minimálně jedenkrát (1x) za rok v případě požadavku kupujícího;

b) kdykoliv v případě bezpečnostního incidentu na straně prodávajícího.

(3) Předmětem auditu bude kontrola dodržování povinností prodávajícího vztahujících se ke kybernetické bezpečnosti a bezpečnosti informací vyplývajících z uzavřené smlouvy včetně příloh, zejména:

a) plnění dohodnutých bezpečnostních opatření definovaných v **příloze č. 2** této smlouvy označené jako „Požadavky na bezpečnostní opatření na straně prodávajícího“;

b) způsob řízení dodavatelů prodávajícího (poddodavatelů);

c) způsob nakládání s daty;

d) způsob identifikace, hlášení a řešení kybernetických bezpečnostních incidentů.

(4) Prodávající je povinen poskytnout potřebnou součinnost a zpřístupnit auditu veškerá data a informace, která mají vliv na předmět smlouvy a jsou potřebná k vyhodnocení auditu.

(5) Kupující ohlásí provedení zákaznického auditu prodávajícímu nejméně 30 dní před požadovaným termínem provedení auditu; v případě zákaznického auditu na podkladě bezpečnostního incidentu musí prodávající umožnit provedení bezodkladně.

(6) Má-li dodavatel zavedený, a nezávislým certifikačním orgánem certifikovaný systém bezpečnosti informací podle normy ČSN ISO/IEC 27001 nebo ČSN/EN 62443 (minimálně pro rozsah poskytovaných služeb), je možné k tomuto při provádění zákaznického auditu přihlédnout, nikoliv však touto certifikací nahradit provedení celého zákaznického auditu.

(7) Kupující je oprávněn pro audit naplnění KB požadavků využít třetí stranu. V případě využití třetí strany bude objednatel odpovídat za třetí stranu, jako by kontrolu prováděl sám.

(8) Prodávající se zavazuje nedostatky zjištěné v rámci zákaznického auditu odstranit ve lhůtě určené v písemném oznámení kupujícího v závislosti na závažnosti zjištění, přičemž je kupující oprávněn požadovat odstranění nejzávažnějších nedostatků do 30 kalendářních dní od jejich oznámení. Nestanoví-li kupující lhůtu v písemném oznámení, zavazují se strany dohodnout na lhůtě pro odstranění nedostatku, která nepřevýší 30 kalendářních dnů.

(9) Prodávající se zavazuje poskytnout zprávu o plnění nápravných opatření u zjištěných nedostatků.

[redacted]

(10) Prodávající je povinen:

a) u významných změn, majících vliv na kybernetickou bezpečnost a bezpečnost informací, dokumentovat jejich řízení, provádět analýzu rizik, přijímat opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami, aktualizovat bezpečnostní dokumentaci, zajistit testování nových dat a zajistit možnost navrácení do původního stavu;

b) informovat kupujícího o výsledcích řízení změn, které mají dopady na plnění předmětu smlouvy;

c) poskytnout kupujícímu, při řízení změn na straně kupujícího, veškerou nezbytnou součinnost při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu;

d) poskytnout kupujícímu při realizaci penetračního testování nebo testování zranitelností veškerou potřebnou součinnost.

(11) Prodávající je povinen informovat kupujícího o bezpečnostních incidentech souvisejících s plněním této smlouvy, které mohou mít vliv na bezpečnost informací (např. napadení mailové komunikace prodávajícího příp. jeho poddodavatelů, napadení sítě/serverů/koncových stanic prodávajícího příp. jeho poddodavatelů, ztráta informací v papírové podobě nebo na nosičích dat apod.):

a) v případě incidentu s možným přímým vlivem na aktiva objednatele – **NEPRODLENĚ**.

b) v ostatních případech do 24 hodin.

(12) Prodávající se zavazuje bezprostředně, nejpozději však do 14 dní po ukončení smlouvy:

a) předat kupujícímu v elektronické podobě veškerá prodávajícímu dostupná provozní, vývojová či testovací data či uživatelské údaje, které vytvořil či používal v rámci plnění dle této smlouvy;

b) předat kupujícímu veškerá hesla, šifrovací klíče, certifikáty a další autentizační prostředky, které prodávajícímu umožnili uživatelský a administrátorský přístup k veškerým datům, databázím, systémům a dalším technickým prostředkům, potřebným pro předmět plnění smlouvy;

c) předat kupujícímu všechna informační aktiva kupujícího, se kterými prodávající pracoval.

(13) O výše uvedených skutečnostech bude vyhotoven předávací protokol se záznamem o předání dat, hesel, klíčů a certifikátů a o prokazatelně bezpečné likvidaci veškerých dat. Kupující je oprávněn provést samostatnou kontrolu a speciální audit bezpečné likvidace veškerých dat u prodávajícího, a to buď prostřednictvím svých vlastních kapacit nebo prostřednictvím externího odborníka či znalce.

(14) Prodávající je povinen:

a) na základě výzvy kupujícího, předat objednateli bez zbytečných odkladů všechna dostupná data, provozní údaje a informace související s plněním předmětu smlouvy v systematizované podobě a ve strojově čitelném formátu;

b) plnit povinnost k mazání dat a k likvidaci technických nosičů a/nebo provozních údajů a/nebo informací a jejich kopií, postupuje v souladu s pravidly pro mazání dat a v souladu se způsoby likvidace technických nosičů informace, provozních údajů, informací a jejich kopií stanovených objednatelem v Pravidla informační a kybernetické bezpečnosti pro dodavatele (PIKYB) zohledňující systém řízení bezpečnosti informací (dále jen „PIKYB“), které jsou dostupné na webových stránkách objednatele www.plzenskateplarenska.cz v sekci „Ke stažení – Dokumenty“. Prodávající podpisem této smlouvy potvrzuje, že se s PIKYB řádně seznámil.

[redacted]

(15) Prodávající je povinen v rozsahu plnění této smlouvy naplnit požadavky ve smyslu zajištění kybernetické bezpečnosti, uvedené v **příloze č. 2** této smlouvy (dále jen „KB požadavky – opatření"), a to nejpozději do 30 kalendářních dnů a následně též po celou jeho dobu plnění.

(16) Prodávající se dále zavazuje:

a) poskytnout na vyžádání kupujícímu dokumenty a obdobné vstupy, které budou prokazovat naplnění KB požadavků;

b) při výkonu své činnosti včas a prokazatelně upozornit kupujícího na zřejmou nevhodnost jeho příkazů či doporučení vztahující se ke KB požadavkům, jejichž následkem může vzniknout újma na informačních aktivech kupujícího nebo nesoulad se zákony či jinými obecně závaznými právními předpisy;

c) neprodleně informovat kupujícího o:

- způsobu řízení rizik na své straně a o zbytkových rizicích souvisejících s plněním smlouvy,
- významné změně ovládání prodávajícího podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných k plnění této smlouvy,
- žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu,
- fyzických osobách přicházejících do kontaktu s důvěrnými informacemi kupujícího;

d) zajistit, že další případní poddodavatelé budou dodržovat veškeré povinnosti vyplývající z této smlouvy v oblasti kybernetické bezpečnosti v plném rozsahu,

e) dodržovat bezpečnostní politiky kupujícího, se kterými byl seznámen.

f) v případě žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu, učiní tak pouze za následujících podmínek: 1. po provedení přezkoumání zákonnosti žádosti, 2. až po vynaložení veškerého úsilí o zabránění zpřístupnění nebo předání dat v rámci možností daných právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána, 3. a pouze v nezbytném rozsahu.

Článek IX.
Autorská a užívací práva

(1) Prodávající se zavazuje k zajištění a předání užívacích práv k jednotlivým dílčím plněním. Užívací práva představují veškerá užívací práva k nehmotným i hmotným statkům, která jsou ze své povahy nutná pro objednatele k nerušenému provozování a údržbě díla, a to včetně oprávnění k výkonu práva užít dílo (licence), know-how a patentů.

Vzhledem k tomu, že součástí díla je i plnění, které může naplňovat znaky autorského díla ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „AZ"), jsou k těmto součástem díla poskytována následující oprávnění:

a) k softwarovým produktům (proprietární/platformní software) považovaným za autorské dílo dle AZ dodávaným jako součást dílčího plnění (dále jen „software") uživatelské licence k užití software k účelu provozu a běžné údržby dílčího plnění a v rozsahu, v jakém uzná prodávající za nezbytné, vhodné či přiměřené. Pro vyloučení pochybností to znamená, že kupující je oprávněn užívat software v potřebném množstevním rozsahu a v územním rozsahu pro Českou republiku, a způsobem, který je v souladu s licenčními podmínkami poskytnutými dodavatelem softwaru. Tyto uživatelské licence jsou uděleny jako nevýhradní a jsou uděleny nejméně na dobu trvání smlouvy a po jejím skončení až do skončení

[redacted]

následujícího kalendářního roku po roce, ve kterém skončila účinnost smlouvy. Licence udělené dle tohoto ustanovení smlouvy se vztahují i na veškeré update a upgrade k software.

b) pro případ, že je výsledkem činnosti prodávajícího dle smlouvy plnění (zejména software nezbytný k fungování (ovládání) díla, s výjimkou software popsaného v předcházející odrážce, a veškerá dokumentace), které podléhá ochraně podle AZ (dále jen „plnění"), neaplikuje se na takové plnění bod výše, ale prodávající poskytuje kupujícímu a kupující od prodávajícího získává oprávnění k výkonu práva plnění užít, a to v rozsahu nezbytném pro řádné užívání plnění kupujícím po celou dobu, kdy bude zboží provozováno. Kupující zejména nabývá od prodávajícího oprávnění k výkonu práva takové plnění užít, a to formou dále uvedeného licenčního ujednání (dále jen „licence"):

- licence je udělena jako nevýhradní, a to ke všem v úvahu přicházejícím způsobům užití plnění, souvisejícím s účelem, ke kterému bylo takové plnění prodávajícím vytvořeno v souladu se smlouvou, a to v rozsahu minimálně nezbytném pro řádné užívání zboží kupujícím;
- licence je udělena jako neodvolatelná, neomezená územním či množstevním rozsahem a za účelem provozování a údržby zboží. Pokud je plněním počítačový program, je prodávající rovněž povinen předat kupujícímu po uplynutí záruční doby veškeré zdrojové kódy (řádně dokumentované, aktualizované a okomentované zdrojové kódy počítačových programů ve spustitelné formě včetně ověřeného postupu nezbytného pro sestavení strojového kódu a koncepční přípravné materiály (zahrnující zejména analýzy a technické designy) k takovému plnění, včetně související dokumentace a to tak, že budou uloženy na k tomu vyhrazených datových prostředcích kupujícího nebo mu budou nejpozději k datu předání plnění, jehož je takové plnění součástí, předány na datovém nosiči;
- licence je dále udělena na dobu určitou (po dobu, po kterou dílo bude provozováno), je nepřevoditelná a nepostupitelná, tj. je udělena bez práva udělení sublicence či postoupení licence jakékoliv třetí osobě; kupující současně není povinen licenci využít, a to ani zčásti;
- povinnost týkající se licence platí pro prodávajícího i v případě dodání části plnění poddodavatelem. Licence je poskytnutá v maximálním rozsahu povoleném platnými právními předpisy; prodávající tímto prohlašuje, že v případě vytvoření plnění zajistí veškerá oprávnění k plnění, zejména, nikoliv však výlučně, že získá veškerá oprávnění autorů či třetích osob k takovému plnění a je oprávněn je poskytnout kupujícímu;
- prodávající dále touto smlouvou uděluje kupujícímu oprávnění po uplynutí záruční doby plnění (počítačový program, ke kterému byly předány zdrojové kódy, i veškerou dokumentaci) upravovat, měnit, zasahovat do něj, spojit jej s jiným dílem, zařazovat jej do souborného díla, to vše do té míry, aby mohlo být zboží provozováno. K provádění uvedených činností je oprávněn samostatně nebo prostřednictvím třetí osoby (dodavatele). Prodávající podpisem této smlouvy potvrzuje, že je oprávněn k poskytnutí uvedených oprávnění kupujícímu, a že tím nedojde k protiprávním zásahům do práv třetích osob (autorů).

(2) Prodávající podpisem smlouvy výslovně prohlašuje, že odměna za veškerá užívací práva poskytnutá kupujícímu dle smlouvy je již zahrnuta v ceně za provedení díla.

(3) Udělení veškerých užívacích práv nelze ze strany prodávajícího vypovědět a na jejich udělení nemá vliv ukončení platnosti smlouvy.

[redacted]

Článek X.
Závěrečná ustanovení

(1) Obě smluvní strany jsou povinny postupovat v průběhu provádění činností v souladu s touto smlouvou a příslušnými právními předpisy, zejména:

- zákonem č. 264/2025 Sb., o kybernetické bezpečnosti v platném znění;
- vyhláškou č. 409/2025 Sb., o bezpečnostních opatřeních, poskytovatele regulované služby v režimu vyšších povinností, ve znění pozdějších předpisů;
- bezpečnostními normami řady ISO 27000 a IEC 62443.

(2) Prodávající je oprávněn odstoupit od smlouvy v případě:

- významné změny kontroly nad prodávajícím dle § 74 a násl. zákona č. 90/2012 Sb., o obchodních korporacích či ekvivalentní postavení;
- změně kontroly nad zásadními aktivy využívanými prodávajícím k plnění dle předmětu smlouvy, která by mohla zásadně ohrozit úroveň kybernetické bezpečnosti kupujícího.

(3) Smluvní strany berou na vědomí, že Plzeňská teplárenská, a.s. je právnickou osobou, v níž má většinovou majetkovou účast územní samosprávný celek, a proto se na tuto smlouvu (dále také jen „smlouva"), v souladu s § 2 odst. 1 písm. n) zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále také jen „ZRS"), vztahuje povinnost uveřejnění prostřednictvím registru smluv (dále také jen „Registr smluv").

(4) Smluvní strany dále prohlašují, že údaje o smluvní straně, se kterou Plzeňská teplárenská, a.s. uzavírá tuto smlouvu, a ceně tvoří obchodní tajemství, a z tohoto důvodu budou tyto údaje (metadata) vyloučeny z uveřejnění v Registru smluv ve smyslu ust. § 5 odst. 6 ZRS.

(5) Smluvní strany se dohodly a souhlasí s tím, že tuto smlouvu uveřejní v Registru smluv pouze Plzeňská teplárenská, a.s., a to ve verzi pro uveřejnění, tj. po znečitelnění údajů (metadat), které tvoří obchodní tajemství, a to nejpozději do 30 dnů po podpisu této smlouvy.

(6) Osobní údaje uvedené v této smlouvě jsou určeny a využity pouze pro účely uzavření tohoto smluvního vztahu a případného plnění vyplývající z předmětu smlouvy; nebudou dále zpracovávány pro jiné účely. Smluvní strany dále prohlašují a zavazují se, že v případě nakládání s osobními údaji při realizaci a plnění této smlouvy budou postupovat v souladu s právem Evropské unie, zejména s nařízením Evropského parlamentu a Rady (EU) ze dne 27. 4. 2016 č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES a příslušnou účinnou a aplikovatelnou národní legislativou vztahující se k ochraně a zpracování osobních údajů.

(7) Tuto smlouvu a její součásti lze měnit jen na základě písemné dohody obou smluvních stran.

(8) Tato smlouva je vyhotovena v elektronické podobě.

(9) Tato smlouva nabývá platnosti datem připojení elektronického podpisu dle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů všemi smluvními stranami do této smlouvy a všech jejích jednotlivých příloh, a účinnosti dnem uveřejnění v Registru smluv.

(10) Práva a povinnosti z této smlouvy vzniklé se řídí českým právním řádem.

[redacted]

(11) Smluvní strany se v souladu s ustanovením § 89a zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů, dohodly na tom, že místně příslušný soud pro rozhodování sporů z této smlouvy je Okresní soud Plzeň-město a v případě, že je pro řízení v prvním stupni věcně příslušný krajský soud, sjednává se jako místně příslušný soud pro rozhodování sporů z této smlouvy Krajský soud v Plzni.

(12) Účastníci si tuto smlouvu přečetli, její obsah je jim srozumitelný a odpovídá jejich pravé a svobodné vůli. Na důkaz toho k ní připojují své podpisy.

Přílohy:

1. Technické zadání vč. příloh
2. Požadavky na bezpečnostní opatření na straně prodávajícího (vč. přílohy č. 1 „Dotazník aplikovaných opatření na straně prodávajícího)“

V Plzni dne:

Kupující:

V [redacted] dne:

Prodávající:

[redacted]

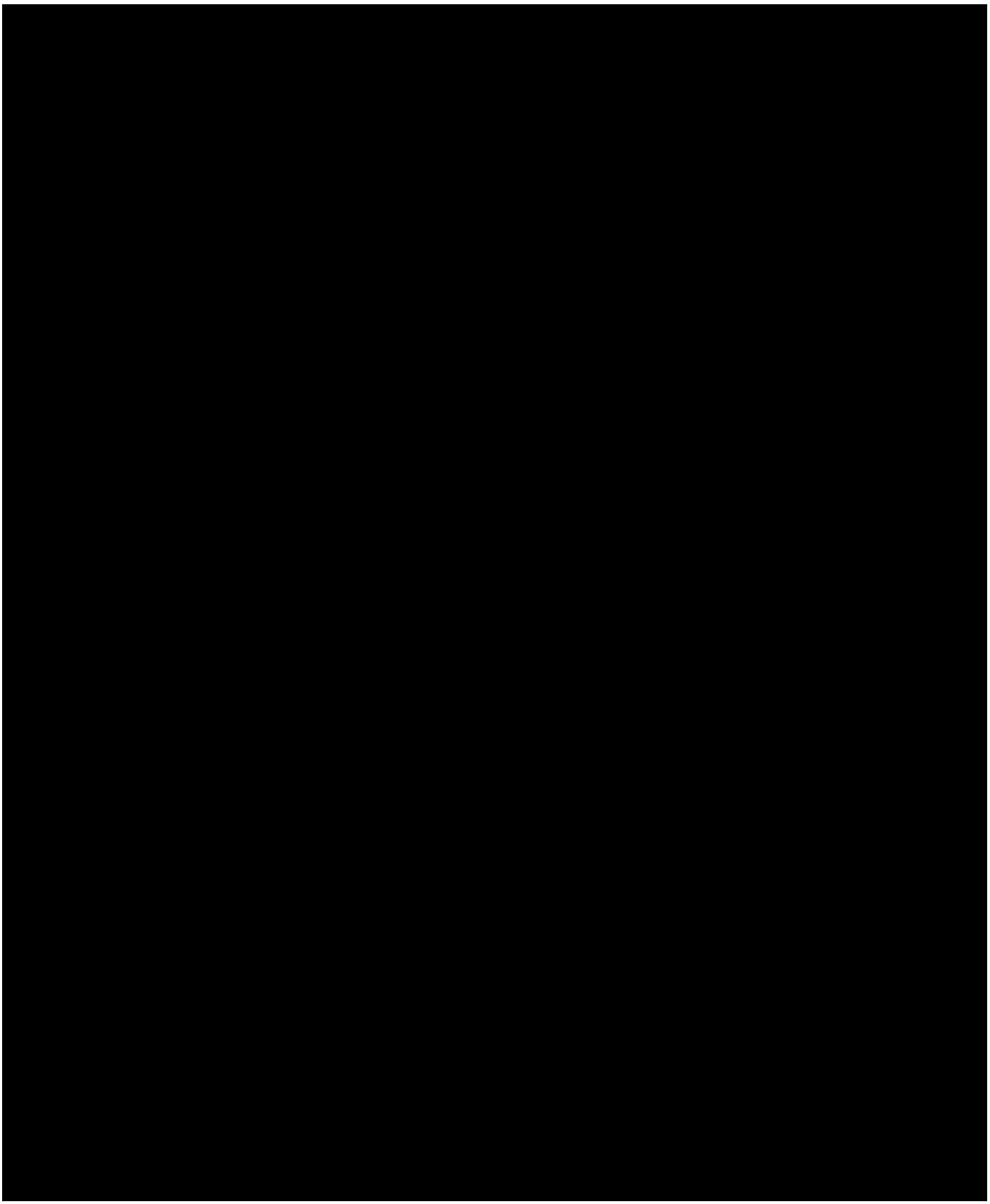
[redacted]

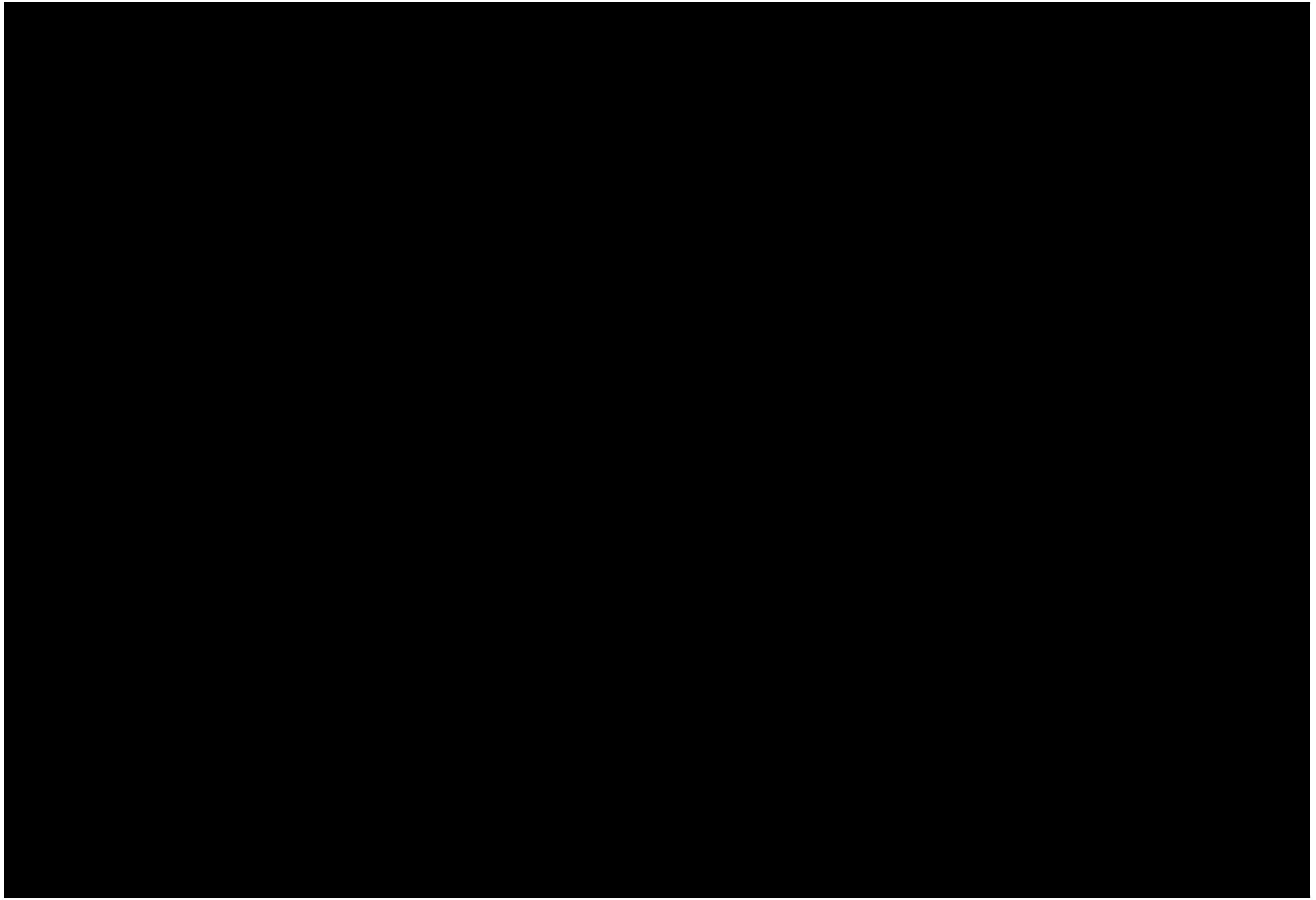
Příloha č. 1

Technické zadání

Obnova bezpečnostních bran (firewally)

Příloha č. 1





POŽADAVKY NA BEZPEČNOSTNÍ OPATŘENÍ NA STRANĚ PRODÁVAJÍCÍHO

Obsah:

1 ZÁKLADNÍ POJMY A ZKRATKY

Pro potřeby této přílohy smlouvy jsou použity následující zkratky a pojmy.

Smlouva	Smlouva o dílo/Kupní smlouva/Rámcová smlouva o poskytování služeb, jejíž přílohou je tento dokument.
Informační bezpečnost	Ochrana informací a informačních systémů před neoprávněným přístupem, užíváním, odhalením, rušením, změnou, inspekcí, záznamem nebo zničením s cílem zabezpečit jejich důvěrnost, integritu a dostupnost.
Kybernetická bezpečnost	Ochrana systémů, sítí a dat v digitálním prostoru před útoky, poškozením nebo neoprávněným přístupem. Zahrnuje implementaci technologií, postupů a strategií na ochranu elektronických informací a infrastruktury.
Prostředky objednatele	Hmotné i nehmotné věci ve vlastnictví nebo nájmu objednatele, které jsou nezbytné k plnění předmětu smlouvy.
Prostředí objednatele	Fyzický perimetr určený ohraničením fyzického prostoru v nájmu nebo majetku objednatele anebo logický perimetr definovaný hraničními prvky informačního/komunikačního systému ve správě nebo majetku objednatele.
Prostředky prodávajícího	Hmotné i nehmotné věci ve vlastnictví nebo nájmu prodávajícího, které jsou nezbytné k plnění předmětu smlouvy.
Prostředí prodávajícího	Fyzický perimetr určený ohraničením fyzického prostoru v nájmu nebo majetku prodávajícího anebo logický perimetr definovaný hraničními prvky informačního/komunikačního systému ve správě nebo majetku prodávajícího.
VoKB	Vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, ve znění pozdějších předpisů.
ZoKB	Zákon č. 264/2025 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.
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.

2 ÚVODNÍ USTANOVENÍ

„Požadavky na bezpečnostní opatření na straně prodávajícího" dle ZoKB a VoKB (dále jen „Bezpečnostní požadavky") je nástrojem pro plnění požadavků na základě:

- ustanovení § 14 odst. 1 písm. a) bod 7 ZoKB,
- ustanovení § 9 VoKB.

3 PŮSOBNOST

Bezpečnostní požadavky musí být uplatněny jak v organizaci, tak i v informačním a komunikačním systému prodávajícího (a jeho poddodavatelů, kteří jsou významnými dodavateli ve smyslu § 2 písm. h) VoKB), minimálně v těch částech, které jsou významné z hlediska zajištění kybernetické bezpečnosti regulované služby a které mohou mít vliv na plnění předmětu díla dle smlouvy.

4 BEZPEČNOSTNÍ OPATŘENÍ

4.1 Systém řízení informační a kybernetické bezpečnosti

V oblasti plnění povinností uvedených v § 3 VoKB, se prodávající zavazuje minimálně:

a) vytvořit a uplatňovat pravidla pro ochranu dat, informací a technických aktiv;
b) vytvořit a udržovat bezpečnostní politiku a bezpečnostní dokumentaci ve vztahu k řízení kybernetické bezpečnosti podle § 3 odst. 1 písm. d) VoKB, která obsahuje hlavní zásady, cíle systému řízení bezpečnosti informací, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací;
c) zajistit vyhodnocování přijatých pravidel a dokumentace, a to alespoň 1x ročně.

4.2 Řízení aktiv

V oblasti plnění povinností uvedených v § 7 VoKB, se prodávající zavazuje minimálně:

a) vytvořit a udržovat seznam s popisem všech technických prostředků (aktiv) jako např. hardware, software, který obsahuje minimálně identifikaci aktiv, jejich popis, vlastníka, umístění a klasifikaci z hlediska důležitosti pro zajištění kybernetické bezpečnosti regulované služby;
b) stanovit pravidla pro jejich používání technických prostředků/aktiv dle bodu 4.2.a);
c) posoudit dopady v souladu s přílohou č. 1 VoKB a toto posouzení na požádání předložit objednateli k nahlédnutí.

4.3 Řízení rizik

V oblasti plnění povinností uvedených v § 8 VoKB, se prodávající zavazuje minimálně:

a) řídit vlastní rizika na základě relevantních hrozeb a zranitelností;
b) alespoň 1x ročně (nebo při významných změnách) vytvořit Zprávu o řízení kybernetických rizik, která bude minimálně pokrývat:
    I. vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok,
    II. identifikaci a hodnocení rizik s vazbou na předmět plnění,
    III. realizovaná bezpečnostní opatření,
    IV. nepokrytá bezpečnostní rizika a návrh opatření,
    V. vyhodnocení bezpečnostních událostí a incidentů,
    VI. aktuální stav souladu prodávajícího s těmito bezpečnostními požadavky.

4.4 Organizační bezpečnost, bezpečnostní role a bezpečnost lidských zdrojů

V oblasti plnění povinností uvedených v § 5, § 10 VoKB, se prodávající zavazuje minimálně:

a) stanovit pravomoci a odpovědnosti v rámci organizace prodávajícího, vedoucí ke zajištění kybernetické bezpečnosti;
b) určit odpovědné osoby zastávajících bezpečnostní role za oblast kybernetické bezpečnosti;
c) stanovit, dodržovat a evidovat plán rozvoje bezpečnostního povědomí/školení, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí a odbornosti pracovníků prodávajícího;
d) účastnit se školení a rozvoje dle požadavků a podkladů předložených objednatelem;
e) poučit uživatele, administrátory a osoby zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostních politikách formou vstupních a pravidelných školení;
f) evidovat přehledy, které obsahují předmět poučení a školení včetně seznamu osob, které poučení a školení absolvovaly.

4.5 Řízení dodavatelů

V oblasti plnění povinností uvedených v § 9 VoKB, se prodávající zavazuje zajistit minimálně:

a) vedení evidence dodavatelů (zejména v rozsahu identifikačních údajů, rozsahu dodávek), jejichž dodávky mají vliv na zajištění informační a kybernetické bezpečnosti;
b) aplikaci bezpečnostních požadavků dle této přílohy na své poddodavatele, jejichž dodávky mají vliv na zajištění informační a kybernetické bezpečnosti;
c) na vyžádání předložit objednateli seznam všech využívaných dodavatelů, jejichž dodávky mají vliv na zajištění informační a kybernetické bezpečnosti.

4.6 Řízení změn

V oblasti plnění povinností uvedených v § 11 VoKB, se prodávající zavazuje minimálně:

a) řídit a evidovat významné změny, za které se považují změny na straně aktiv prodávajícího, které mají nebo mohou mít vliv na kybernetickou bezpečnost a představují vysoké riziko pro plnění předmětu smlouvy;
b) přijímat bezpečnostní opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami;
c) v souvislosti se změnami aktualizovat bezpečnostní a provozní dokumentaci;
d) "Vysoké riziko" v tomto kontextu označuje jakoukoli situaci nebo změnu, která může významně narušit dodávané služby, zvýšit pravděpodobnost úspěšného kybernetického útoku, vést k nesouladu s právními normami, způsobit významné finanční ztráty nebo závislost na nespolehlivých třetích stranách. Zahrnuje také situace, kdy jsou potřebné významné změny v systémech, které by mohly vést k novým nezamýšleným zranitelnostem.

4.7 Řízení přístupu

V oblasti plnění povinností uvedených v § 13 VoKB, prodávající minimálně:

a) řídí přístup na základě skupin nebo rolí (RBAC);
b) přiděluje každému uživateli i administrátorovi přistupujícímu k aktivům přístupová práva a oprávnění pouze v rozsahu nezbytně nutném k výkonu práce a jedinečný identifikátor daného typu účtu, přičemž **odděluje uživatelské a administrátorské účty** jedné osoby;
c) řídí identifikátory, přístupová práva a oprávnění účtů technických aktiv;
d) zavádí bezpečnostní opatření pro řízení přístupu technických aktiv dle písm. c);

e) zavádí bezpečnostní opatření pro bezpečné používání mobilních zařízení a jiných obdobných technických aktiv; tato opatření uplatní i pro technická aktiva, která nejsou v jeho správě, pokud jsou využívána při plnění;

f) omezuje a kontroluje používání programových prostředků a vybavení schopných překonat systémové nebo aplikační kontroly (např. nástroje pro eskalaci oprávnění, „break-glass" přístupy);

g) přiděluje a odebírá přístupová práva a oprávnění v souladu s platnou politikou řízení přístupu;

h) **provádí pravidelné přezkoumání** všech přístupových práv a oprávnění včetně rozdělení do skupin a rolí;

i) **zajišťuje bezodkladnou změnu** přístupových práv a oprávnění při změně pozice nebo zařazení uživatele na základě skupin a rolí;

j) **zajišťuje deaktivaci účtů a bezodkladné odebrání či změnu** přístupových práv a oprávnění při ukončení nebo změně smluvního vztahu, na jehož základě byl zřízen přístup k aktivům (včetně zaměstnanců a poddodavatelů prodávajícího);

k) **dokumentuje** přidělování a odebírání přístupových práv a oprávnění;

l) **využívá nástroj** pro správu a ověřování identity podle § 19 VoKB a nástroj pro řízení přístupových práv a oprávnění podle § 20 VoKB a tyto nástroje aplikuje na veškeré přístupy použité při plnění této smlouvy.

4.8 Akvizice, vývoj a údržba

V oblasti plnění povinností uvedených v § 12 VoKB, se prodávající zavazuje minimálně:

a) zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které prodávající používá nebo nasazuje;

b) zajistit, že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování řešení a/nebo které jsou specifikovány výslovně ve smlouvě (zejména, že řešení nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.).

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

a) dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru definované;

b) zajistit, že do produkčního bude dodáván jen předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování předmětu plnění;

c) zajistit řízení verzí zdrojového kódu;

d) zajistit zálohování zdrojového kódu;

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

4.9 Zvládání kybernetických bezpečnostních incidentů

V oblasti plnění povinností uvedených v § 15 VoKB, se prodávající zavazuje zajistit minimálně:

a) stanovení a aplikování postupů pro detekci, hlášení, vyhodnocení a řešení kybernetických bezpečnostních incidentů na komunikační a informační infrastruktuře prodávajícího, včetně klasifikace incidentů podle jejich závažnosti a dopadu na regulovanou službu;

b) proces včasného informování osob zastávajících bezpečnostní role o vzniku kybernetických bezpečnostních incidentů, včetně definice lhůt pro hlášení v závislosti na závažnosti incidentu;

c) evidenci bezpečnostní události v rozsahu:

I. datum a čas zjištění,
II. povaha a popis události,
III. zdroje události,
IV. cíle/oběti události,
V. potenciální dopad na regulovanou službu a aktiva,
VI. přijatá opatření k řešení incidentu,
VII. stav řešení incidentu;

d) bez zbytečného odkladu realizaci nápravných a preventivních opatření k minimalizaci rizika kybernetického bezpečnostního incidentu souvisejícího s předmětem smlouvy, včetně analýzy příčin a přijetí opatření k zamezení opakování.

Prodávající bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení těchto Bezpečnostních požadavků, jehož příčina je na straně prodávajícího, nebude posuzován jako okolnost vylučující odpovědnost prodávajícího.

4.10 Kontrola a audit

V oblasti plnění povinností uvedených v § 16 VoKB, se prodávající zavazuje minimálně:

a) pravidelně provádět kontrolu/audit plnění opatření uvedených v tomto dokumentu;
b) vyhradit si právo provést kontrolu/audit plněné bezpečnostních požadavků u svých poddodavatelů.

4.11 Kontinuita činnosti

V oblasti plnění povinností uvedených v § 15 VoKB, se prodávající zavazuje minimálně:

a) stanovit minimální úroveň poskytovaných služeb, zajišťující plnění předmětu díla dle smlouvy;
b) vyhodnotit možné dopady kybernetických bezpečnostních incidentů na zajištění kontinuity činnosti;
c) vypracovat, aktualizovat a testovat havarijní plány pro obnovu informačního a komunikačního systému.

4.12 Fyzická bezpečnost

V oblasti plnění povinností uvedených v § 17 VoKB, se prodávající zavazuje minimálně:

a) stanovit fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány a zpracovány informace a umístěna technická aktiva informačního a komunikačního systému;
b) přijmout nezbytná opatření a použít prostředky fyzické bezpečnosti, pro zamezení neoprávněnému fyzickému přístupu do bezpečnostního perimetru dle bodu a);
c) v rozsahu předmětu plnění zajistit fyzické zabezpečení instalačních, záložních nebo archivních médií a dokumentace v souladu s požadavky na bezpečné nakládání s informacemi definovanými v souladu s Pravidla informační a kybernetické bezpečnosti pro dodavatele (PIKYB) zohledňující systém řízení bezpečnosti informací;
d) povinnosti dle tohoto článku se vztahují na aktiva **objednatele** i **prodávajícího**, k nimž prodávající nebo osoby jednající jeho jménem získají přístup při plnění této smlouvy.

4.13 Bezpečnost komunikačních sítí

V oblasti plnění povinností uvedených v § 18 VoKB, se prodávající zavazuje zajistit minimálně:

a) vhodnou segmentaci komunikační sítě, včetně oddělení provozního, zálohovacího, vývojového, testovacího, administrátorského a jiného specifického prostředí, a vedení

aktuální dokumentace topologie komunikační sítě a infrastruktury; řízení komunikace, blokování nežádoucí komunikace v rámci komunikační sítě a na jejím perimetru;

b) vhodným způsobem zabezpečit bezdrátové technologie a případný vzdálený přístup do komunikační sítě;

c) využití nástrojů pro zajištění ochrany integrity komunikační sítě;

d) dokumentaci a průběžnou aktualizaci všech opatření přijatých podle tohoto článku.

4.14 Správa a ověřování identit, řízení přístupových oprávnění

V oblasti plnění povinností uvedených v § 19 a § 20 VoKB, se prodávající zavazuje zajistit minimálně:

a) použití vhodného nástroje nebo procesu pro správu a ověření identit uživatelů, který zajistí mj. uložení autentizačních údajů ve formě odolné vůči zneužití;

b) stanovení požadavků na dostatečnou sílu hesla pro uživatele a administrátory a délku jeho platnosti;

c) stanovení pravidel automatického zablokování přístupu v případě opakovaného neúspěšného přihlášení a obdobných podezřelých aktivit.

4.15 Detekce kybernetických bezpečnostních událostí

a) V oblasti plnění povinností uvedených v § 21 vyhlášky o kybernetické bezpečnosti se **prodávající** zavazuje zajistit minimálně nepřetržitou a automatickou ochranu před škodlivým kódem na všech relevantních prvcích informačního systému (včetně koncových zařízení, serverů, mobilních zařízení, síťových prvků a dalších technických aktiv), s využitím centrálně spravovaného nástroje pro detekci kybernetických bezpečnostních událostí;

b) pravidelnou a bezodkladnou aktualizaci nástroje a jeho detekčních mechanismů, včetně virových databází, detekčních pravidel a konfigurace, tak aby byla zajištěna aktuální ochrana proti novým typům hrozeb;

c) ověřování a kontrolu přenášených dat v rámci komunikační sítě, mezi sítěmi a na síťovém perimetru, včetně aktivního blokování nežádoucí komunikace;

d) vhodnou ochranu před škodlivým kódem u zařízení, na kterých není možné nainstalovat nebo spustit standardní antivirovou ochranu, prostřednictvím alternativních opatření (např. aplikační whitelisting, sandboxing, omezení komunikace, pravidelný monitoring integrity);

e) řízení a sledování používání výměnných zařízení a datových nosičů, včetně:
   a. řízení oprávnění ke spouštění kódu,
   b. řízení automatického spouštění obsahu na výměnných médiích,
   c. vedení evidence a kontroly připojování výměnných médií a zařízení;

f) stanovení pravidel pro používání výměnných paměťových médií a dalších přenosných datových zařízení v souladu s politikou bezpečného nakládání s informacemi;

g) sledování a detekci kybernetických bezpečnostních událostí vycházejících z chování technických aktiv, administrátorů a uživatelů, a jejich předávání do systému detekce a reakce na incidenty podle § 22 VoKB;

h) řízení a sledování komunikace aplikací, služeb a procesů, které mohou být zdrojem nebo cílem škodlivého kódu.

4.16 Záznamy událostí v informačním systému

V oblasti plnění povinností uvedených v § 22 VoKB, se prodávající zavazuje zajistit minimálně:

a) zaznamenávat důležité bezpečnostní a provozní údaje technických aktiv informačního a komunikačního systému;

b) zaznamenávat činnosti uživatelů informačního a komunikačního systému důležité z hlediska bezpečnosti a ochrany informací;
c) používat časovou synchronizaci technických aktiv;
d) uchovávat záznamy událostí informačního a komunikačního systému nejméně dobu 18 měsíců ve formě odolné proti modifikaci.

4.17 Vyhodnocení kybernetických bezpečnostních událostí

V oblasti plnění povinností uvedených v § 23 VoKB, se prodávající zavazuje zajistit minimálně:

a) ověření a kontrolu přenášených dat jak uvnitř, tak vně informačního a komunikačního systému;
b) blokování nežádoucí komunikace;
c) detekci kybernetických bezpečnostních událostí na technických aktivech informačního a komunikačního systému, přiměřeně s ohledem na jejich důležitost;
d) proces včasného informování osob zastávající bezpečnostní role o vzniku kybernetických bezpečnostních událostí.

4.18 Aplikační bezpečnost

V oblasti plnění povinností uvedených v § 24 VoKB, se prodávající zavazuje zajistit minimálně:

a) důkladné plánování bezpečnostních opatření pro veškeré aplikace a technická aktiva využívaná při plnění této smlouvy, s ohledem na dostupné zdroje, rizika a vazby mezi aktivy;
b) analýzu hrozeb a zranitelností aplikací ve všech fázích jejich životního cyklu, včetně návrhu, vývoje, testování, provozu a údržby, s cílem identifikovat a minimalizovat rizika;
c) používání pouze takových technických aktiv a aplikací, které jsou výrobcem, dodavatelem nebo jinou osobou podporovány, a zajištění aplikování všech schválených bezpečnostních aktualizací;
d) v případech, kdy není možné zajistit podporu výrobce nebo aplikaci poslední bezpečnostní aktualizace, zavedení náhradních opatření zaručujících obdobnou nebo vyšší úroveň bezpečnosti a vedení evidence těchto technických aktiv, včetně odůvodnění a přijatých kompenzačních opatření;
e) zabezpečení aplikací, informací, transakcí a přenášených identifikátorů relací před neoprávněnou činností a popřením provedených činností;
f) pravidelné skenování zranitelností technických aktiv a aplikací využívaných v rámci poskytovaných služeb:
    a. z vnitřní i vnější komunikační sítě,
    b. nejméně jednou ročně,
    c. s vyhodnocením výsledků v rámci řízení rizik a následným zavedením odpovídajících bezpečnostních opatření;
g) provádění penetračního testování technických aktiv a aplikací:
    a. z vnitřní i vnější komunikační sítě,
    b. před uvedením do provozu,
    c. po každé významné změně podle § 11 odst. 3 VoKB,
    d. pravidelně alespoň jednou za 2 roky,
    e. v odůvodněných případech možnost rozdělit penetrační testování do systematických celků, přičemž celý rozsah musí být dokončen nejpozději do 5 let;
h) evidenci všech provedených testů a jejich výsledků, včetně termínu provedení a identifikace fyzických osob, které testování prováděly, a zajištění nápravných opatření na základě zjištěných zranitelností;

i) opakované otestování zjištěných nálezů z provedeného skenování nebo penetračního testování za účelem ověření účinnosti zavedených bezpečnostních opatření;
j) pravidelné testování aplikací ve všech fázích vývoje na přítomnost zranitelností a potenciálních hrozeb, včetně automatizovaných testů a kontrol bezpečnostních funkcí;
k) udržování a aktualizaci bezpečnostních opatření aplikací po celou dobu jejich životního cyklu, včetně revizí bezpečnostních postupů a reakce na nově identifikovaná rizika.

4.19 Kryptografické algoritmy

V oblasti plnění povinností uvedených v § 25 VoKB, se prodávající zavazuje zajistit minimálně:

a) používat kryptografické prostředky tam, kde je to žádoucí, smysluplné, účelné a technicky proveditelné;
b) používat odolné kryptografické algoritmy a klíče.

4.20 Dostupnost regulované služby

V oblasti plnění povinností uvedených v § 26 VoKB, se prodávající zavazuje zajistit minimálně:

a) stálou dostupnost všech nezbytných prostředků a informací potřebných k řádnému plnění smlouvy;
b) včasnou nápravu jakýchkoli výpadků nebo přerušení, které by mohly ohrozit plnění smluvních povinností;
c) pravidelné testování integrity, dostupnosti a obnovitelnosti.

Příloha č. 1 – Dotazník aplikovaných opatření na straně prodávajícího

Dotazník aplikovaných opatření na straně prodávajího