




**PLZEŇSKÁ  
TEPLÁRENSKÁ**

Více než energie 



## **SMLOUVA O POSKYTOVÁNÍ SLUŽEB ZAJIŠTĚNÍ KYBERNETICKÉ BEZPEČNOSTI**

**číslo smlouvy objednatele: D2026/0184**

(dále také jako „smlouva“)

Smluvní strany:

Objednatel:

**Plzeňská teplárenská, a.s.**

se sídlem: Plzeň, Doubravecká 2760/1, Východní Předměstí, PSČ 301 00

zapsaný v OR vedeném Krajským soudem v Plzni pod sp. zn. B 392

zastoupený

IČ: 49790480

DIČ: CZ49790480

ID datové schránky: 4ixcgp7

Bankovní spojení:

Číslo účtu:

(dále jen „Objednatel“)

a

Poskytovatel:

(dále jen „Poskytovatel“)

(společně také jako „Smluvní strany“)

uzavřely tuto dohodu v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, v platném znění (dále jen „Občanský zákoník“)

(dále jen “Smlouva“)

Strany, vědomy si svých závazků v této Smlouvě obsažených a s úmyslem být touto Smlouvou vázány, dohodly se na následujícím znění Smlouvy:

## I. PŘEDMĚT SMLOUVY

- 1.1 Předmětem této Smlouvy je závazek Poskytovatele podle podmínek sjednaných v této Smlouvě poskytovat Objednateli a Oprávněným subjektům, jejichž seznam je uveden v Příloze č. 1 této Smlouvy, služby kybernetické bezpečnosti spočívající zejména v zajištění odborných činností a podpory nezbytné k plnění povinností, které na Objednatele a/nebo Oprávněné subjekty dopadají dle zákona č. 264/2025 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, a souvisejících prováděcích právních předpisů a metodických či závazných opatření vydávaných příslušnými orgány veřejné moci, zejména Národním úřadem pro kybernetickou a informační bezpečnost. Konkrétní rozsah a obsah poskytovaných služeb kybernetické bezpečnosti je vymezen v Příloze č. 2 této Smlouvy (dále jen „Služby“). V případě rozporu mezi ustanoveními této Smlouvy a Přílohou č. 2 této Smlouvy má přednost vymezení uvedené v Příloze č. 2 této Smlouvy.

- 1.2 Poskytovatel výslovně prohlašuje, že jím poskytované plnění dle této Smlouvy odpovídá všem požadavkům vyplývajícím z platných právních předpisů či příslušných platných technických norem, které se na plnění vztahují.

## II. ZPŮSOB, TERMÍN A MÍSTO POSKYTOVÁNÍ SLUŽEB

- 2.1 Poskytovatel je povinen poskytovat Služby po celou dobu trvání této Smlouvy. Poskytovatel je povinen reagovat na potřeby Objednatele v takovém časovém určení, jaké vyžaduje povaha uloženého úkolu, popř. lhůty určené právními předpisy.
- 2.2 Poskytovatel je při poskytování Služeb povinen postupovat s potřebnou odbornou péčí, samostatně, podle svých nejlepších znalostí a schopností, přičemž je při své činnosti povinen sledovat a chránit zájmy a dobré jméno Objednatele a postupovat v souladu s jeho pokyny, pokud tyto pokyny nejsou v rozporu s obecně závaznými právními předpisy nebo zájmy Objednatele. V případě nevhodných pokynů Objednatele je Poskytovatel povinen na nevhodnost těchto pokynů Objednatele prokazatelně upozornit, v opačném případě nese Poskytovatel odpovědnost za vady a za škodu, které v důsledku nevhodných pokynů Objednatele Objednateli vznikly.
- 2.3 Poskytovatel se zavazuje informovat Objednatele o všech skutečnostech mající vliv na plnění dle této Smlouvy.
- 2.4 Poskytovatel se zavazuje zajistit, že pověřená osoba Poskytovatele bude Služby dle této Smlouvy poskytovat osobně v sídle Objednatele nebo prostřednictvím prostředků komunikace na dálku. Fyzická přítomnost pověřené osoby Poskytovatele u Objednatele bude zajištěna podle věcné potřeby, zejména pro účely osobních jednání, workshopů, auditů, kontrolních úkonů, šetření kybernetických bezpečnostních incidentů nebo činností vyžadujících fyzický přístup do prostor či k prostředkům Objednatele. V případě, že Objednatel bude požadovat fyzickou přítomnost pracovníka Poskytovatele, je povinen o tom Poskytovatele v dostatečném časovém předstihu informovat.
- 2.5 Objednatel se zavazuje k aktivní a odborné součinnosti s Poskytovatelem v oblasti kybernetické bezpečnosti. Za tímto účelem poskytne Objednatel Poskytovateli veškerou jemu dostupnou dokumentaci a informace nezbytné k řádnému plnění této Smlouvy, zejména podklady k systémům, infrastruktuře a souvisejícím procesům, a zajistí součinnost při identifikaci a hodnocení rizik. Je-li to s ohledem na povahu předmětu plnění nezbytné, zajistí Objednatel Poskytovateli odpovídající přístup k příslušným systémům a infrastruktuře, případně i přístup na příslušná pracoviště Objednatele, a dále zajistí dostatečný čas a aktivní účast relevantních zaměstnanců či jiných pověřených osob na vyžádání Poskytovatele. Objednatel se zavazuje dodržovat standardy a postupy stanovené v oblasti kybernetické bezpečnosti podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti v platném znění (dále jen „ZoKB“) a vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností v platném znění (dále jen „VoKB“) a mezinárodních norem řady ISO 27000 a IEC 62443, a poskytovat Poskytovateli součinnost nezbytnou k řádnému plnění jeho povinností dle této Smlouvy. Poskytovatel se zavazuje požádat Objednatele včas o potřebnou součinnost a při vstupu a pohybu v objektech Objednatele dodržovat příslušné bezpečnostní předpisy, se kterými byl předem seznámen.
- 2.6 Smluvní strany se dohodly na pověřených osobách ze strany Poskytovatele pro plnění předmětu této Smlouvy definovaných v Příloze č. 3 této Smlouvy. Poskytovatel je oprávněn jednostranně změnit pověřenou osobu uvedenou v Příloze č. 3 této Smlouvy, a to písemným oznámením doručeným Objednateli.
- 2.7 Smluvní strany se dohodly, že na plnění předmětu Smlouvy se může podílet třetí strana, se kterou má Poskytovatel uzavřenou Smlouvu. Poskytovatel je povinen o této skutečnosti Objednatele

předem informovat a vyžádat si jeho předchozí písemný souhlas. Předchozího souhlasu není třeba, hrozí-li bezprostřední vznik škody a tímto postupem dochází k jejímu odvrácení. Plní-li předmět Smlouvy třetí osoba, odpovídá za její plnění Poskytovatel, jako by plnil sám.

### III. CENA A PLATEBNÍ PODMÍNKY

- 3.1 Smluvní strany se dohodly, že měsíční paušální cena za poskytování Služeb podle této Smlouvy činí [redacted] (dále jen „Paušál“). Sjednaná odměna neobsahuje daň z přidané hodnoty. K paušální ceně se tato daň připočítá v sazbě daně podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění platném v den uskutečnění zdanitelného plnění.
- 3.2 Smluvní strany se zároveň dohodly, že Paušál uvedený v článku 3.1 této Smlouvy není konečný, neboť se sestává zejména ze mzdových, administrativních a dalších nákladů na poskytování Služeb podle této Smlouvy (dále jen „Skutečné náklady“). Vždy k 1. 3. bude vyhodnocena celková výše Skutečných nákladů na poskytované Služby za předchozí kalendářní rok, a to tak, že Poskytovatel předloží Objednateli vyčíslení Skutečných nákladů spojených s poskytováním Služeb dle této Smlouvy. K celkovým nákladům bude připočten zisk ve výši [redacted].
- Případný rozdíl mezi souhrnem uhrazených Paušálů a Skutečnými náklady včetně uvedeného zisku bude v případě nedoplatku fakturován samostatným daňovým dokladem (fakturou). Případný přeplatek bude v příslušné výši započten na platby v dalších měsících až do úplného započtení.
- V případě, že by Skutečné náklady za poskytování Služeb dle této Smlouvy překročily o více než [redacted] cenu vyplývající z Paušálu dle článku 3.1 této Smlouvy, tj. průměrná cena za služby na měsíc by byla vyšší než [Paušál × [redacted] Kč, je třeba toto navýšení předem odsouhlasit Objednatelům. Bez takového odsouhlasení je Poskytovatel oprávněn účtovat nejvýše částku odpovídající tomuto limitu. Sjednaná odměna neobsahuje daň z přidané hodnoty. K paušální ceně se tato daň připočítá v sazbě podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění platném v den uskutečnění zdanitelného plnění.
- 3.3 Poskytovatel se zavazuje vést průkaznou evidenci Skutečných nákladů vztahujících se k plnění dle této Smlouvy a na vyžádání umožnit Objednatelům nahlédnout do podkladů v rozsahu nezbytném pro ověření vyúčtování.
- 3.4 Poskytovatel je oprávněn jednostranně navýšit Paušál za poskytované Služby uvedený v článku 3.1. této Smlouvy vždy k 1. 3. kalendářního roku, a to maximálně o [redacted] proti předchozí ceně. Navýšení vyšší než o [redacted] je možné jen na základě písemného dodatku k této Smlouvě. Navýšení bude odpovídat vyúčtování ceny za Služby za předchozí kalendářní rok s tím, že v tomto navýšení nebudou zohledněny mimořádné výdaje (např. mimořádná školení). Objednatel je oprávněn nejpozději do 21 dní ode dne obdržení informace o navýšení ceny oznámit Poskytovateli, že s navýšením ceny nesouhlasí. V takovém případě vstoupí Smluvní strany do jednání o podmínkách dalšího pokračování této Smlouvy.
- 3.5 Platby budou prováděny měsíčně na základě faktur vystavených Poskytovatelem do 5. dne kalendářního měsíce následujícího po kalendářním měsíci, za nějž je fakturováno. Vystavený daňový doklad bude zaslán na e-mailovou adresu Objednatele: [redacted]
- 3.6 Poskytované Služby budou Poskytovatelem fakturovány vždy k poslednímu dni příslušného měsíce. Poskytovatel vystaví faktury (daňové doklady) nejpozději do 15. dne následujícího kalendářního měsíce.
- 3.7 Faktura (daňový doklad) vystavená Poskytovatelem musí kromě náležitostí požadovaných obecně závaznými právními předpisy obsahovat také číslo smlouvy Objednatele, č. objednávky N26/1385, údaj o době splatnosti faktury uvedený v souladu s touto Smlouvou a dále vyčíslení

zvlášť ceny Služeb bez DPH, zvlášť DPH a cenu Služeb včetně DPH.

- 3.8 Smluvní strany se dohodly na lhůtě splatnosti faktury v délce třiceti (30) kalendářních dnů ode dne doručení faktury Objednateli. Cena za poskytnuté Služby se považuje za uhrazenou okamžikem připsání fakturované ceny za poskytnuté Služby na bankovní účet Poskytovatele.
- 3.9 K uvedeným cenám bude účtováno DPH dle platných právních předpisů.
- 3.10 Pokud faktura nebude mít všechny sjednané náležitosti nebo bude chybně vystavena, je Objednatel oprávněn ji vrátit a nedostává se tím do prodlení s platbou. Objednatel je oprávněn fakturu vrátit též, pokud na faktuře bude uvedeno jiné číslo účtu, než je uvedeno výše v této Smlouvě. Objednatel není oprávněn vrátit fakturu pouze v případě, bude-li na ní uveden jiný bankovní účet Poskytovatele zveřejněný správcem daně v registru plátců DPH a přílohou faktury bude prohlášení odpovědné osoby Poskytovatele, že žádá provést úhradu na účet uvedený na faktuře.
- 3.11 Poskytovatel prohlašuje, že bankovní účet Poskytovatele uvedený v této Smlouvě je v souladu se zákonem č. 235/2004 Sb., v platném znění, účtem zveřejněným správcem daně v registru plátců DPH.
- 3.12 Poskytovatel prohlašuje, že ke dni podpisu této Smlouvy není vůči němu vydáno správcem daně rozhodnutí o nespolehlivém plátcu ve smyslu § 106a zákona č. 235/2004 Sb., v platném znění, že takové řízení není vůči němu zahájeno ani vedeno a že u něho nejsou dány podmínky pro zahájení řízení o nespolehlivosti plátce u příslušného správce daně.
- 3.13 Poskytovatel se zavazuje, že pokud přestanou platit skutečnosti uvedené v odst. 8. nebo 9. tohoto článku, neprodleně, tj. do 5 dnů ode dne, kdy skutečnost nastala, tuto skutečnost oznámí Objednateli a uzavře s ním dodatek ke Smlouvě. Obsahem takového dodatku bude nastavení postupů předjímaných § 109a zákona č. 235/2004 Sb., v platném znění, nebo sjednání práva Objednatele zadržet částku odpovídající výši DPH do doby splnění daňové povinnosti Poskytovatelem.
- 3.14 Poskytovatel souhlasí s tím, že pokud Objednatel zjistí, že neplatí prohlášení uvedená v odst. 8. nebo 9. tohoto článku, je do doby uzavření dodatku k této Smlouvě oprávněn zadržet částku odpovídající výši DPH do doby splnění daňové povinnosti Poskytovatelem.

#### **IV. PLATNOST SMLOUVY A Odstoupení od Smlouvy**

- 4.1 Tato Smlouva se uzavírá na dobu 3 let. Kterákoli Smluvní strana je oprávněna vypovědět tuto Smlouvu, a to bez uvedení důvodu s dvanáctiměsíční výpovědní lhůtou počínající běžet prvním dnem měsíce následujícího po doručení výpovědi.
- 4.2 Kromě možnosti podání výpovědi bez uvedení důvodu může být Smlouva ukončena písemnou dohodou Smluvních stran.
- 4.3 Každá ze Smluvních stran je oprávněna od této Smlouvy odstoupit, stanoví-li tak Smlouva nebo poruší-li druhá Smluvní strana Smlouvu podstatným způsobem ve smyslu ustanovení § 2001 a násl. Občanského zákoníku.

#### **V. ODPOVĚDNOST ZA ŠKODU, OMEZENÍ NÁHRADY ŠKODY, VYŠŠÍ MOC**

- 5.1 Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škod a k minimalizaci vzniklých škod.

- 5.2 Poskytovatel odpovídá Objednateli za škody, které vyplývají nebo jsou výsledkem porušení právních předpisů, norem či smluvních povinností Poskytovatelem v souvislosti s výkonem činností dle této Smlouvy.
- 5.3 Žádná ze Smluvních stran není odpovědná za případné škody způsobené prodlením s plněním závazků druhé Smluvní strany, pokud takové prodlení nebylo přímo způsobeno zanedbáním nebo úmyslným pochybením této strany. Nedodržení závazků dle článku 2.5 této Smlouvy ze strany Objednatele může vést k jeho částečné nebo plné odpovědnosti za škody, za které Poskytovatel nesmí být postihován.
- 5.4 Žádná ze Smluvních stran není odpovědná za prodlení způsobené okolnostmi vylučujícími odpovědnost (vyšší moc). Za okolnosti vylučující odpovědnost se považuje překážka, jež nastala nezávisle na vůli povinné strany a brání jí ve splnění její povinnosti, jestliže nelze rozumně předpokládat, že by povinná strana tuto překážku nebo její následky odvrátila nebo překonala (např. živelné pohromy, stávky, výpadek el. proudu apod.). Odpovědnost nevylučuje překážka, která vznikla teprve v době, kdy povinná strana byla v prodlení s plněním své povinnosti nebo vznikla z jejích hospodářských poměrů. Účinky vylučující odpovědnost jsou omezeny pouze na dobu, dokud trvá překážka, s níž jsou tyto povinnosti spojeny.
- 5.5 Smluvní strany se zavazují upozornit druhou Smluvní stranu bez zbytečného odkladu na vzniklé okolnosti vylučující odpovědnost bránící řádnému plnění Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání okolnosti vylučujících odpovědnost.

## VI. PRÁVA DUŠEVNÍHO VLASTNICTVÍ

- 6.1 Poskytovatel se zavazuje, že při poskytování Služeb neporuší práva třetích osob, která těmto osobám mohou plynout z práv k duševnímu vlastnictví, zejména z autorských práv a práv průmyslového vlastnictví. Poskytovatel se zavazuje, že Objednateli uhradí veškeré náklady, výdaje, škody a majetkovou i nemajetkovou újmu, které Objednateli vzniknou v důsledku uplatnění práv třetích osob vůči Objednateli v souvislosti s porušením povinnosti Poskytovatele dle předchozí věty.
- 6.2 Bude-li výsledkem nebo součástí poskytování Služeb i dílo, které je předmětem autorských práv, práv souvisejících s právem autorským či práv pořizovatele k jím pořízené databázi, poskytuje Poskytovatel jako autor ode dne předání díla na neomezenou dobu Objednateli pro území celého světa výhradní licenci k užití díla všemi způsoby užití v neomezeném rozsahu, přičemž výše odměny za poskytnutí licence je již zahrnuta v ceně předmětu plnění.

## VII. POVINNOST MLČENLIVOSTI

- 7.1 Smluvní strany se zavazují zachovávat ve vztahu ke třetím osobám mlčenlivost o informacích, které při plnění této Smlouvy získají od jiné Smluvní strany nebo o ní či jeho zaměstnancích a spolupracovnících a nesmí je zpřístupnit bez písemného souhlasu této Smluvní strany žádné třetí osobě ani je používat v rozporu s účelem této Smlouvy, ledaže se jedná o:
- a) informace, které jsou veřejně přístupné, nebo
  - b) případ, kdy je zpřístupnění informace vyžadováno zákonem nebo závazným rozhodnutím oprávněného orgánu.
- 7.2 Poskytovatel je povinen zavázat povinností mlčenlivosti podle článku 7.1 této Smlouvy všechny osoby (včetně třetích stran uvedených v Příloze č. 3 této Smlouvy), které se budou podílet na poskytování plnění Objednateli dle této Smlouvy.

- 7.3 Za porušení povinnosti mlčenlivosti osobami, které se budou podílet na poskytování plnění dle této Smlouvy, odpovídá Poskytovatel, jako by povinnost porušil sám.

## VIII. OSTATNÍ UJEDNÁNÍ

- 8.1 Smluvní strany jsou povinny bez zbytečného odkladu oznámit druhé straně změnu údajů v záhlaví Smlouvy.
- 8.2 Poskytovatel není bez předchozího písemného souhlasu všech Objednatelů oprávněn postoupit práva a povinnosti z této Smlouvy na třetí osobu. Žádný z Objednatelů není bez předchozího písemného souhlasu Poskytovatele oprávněn postoupit práva a povinnosti z této Smlouvy na třetí osobu.
- 8.3 Každá ze Smluvních stran je povinna dokumenty související s poskytováním Služeb dle této Smlouvy uchovávat nejméně po dobu deseti (10) let od konce účetního období, ve kterém došlo k zaplacení poslední části ceny Služby, popř. k poslednímu zdanitelnému plnění dle této Smlouvy, a to zejména pro účely kontroly oprávněnými kontrolními orgány.

## IX. BEZPEČNOST PRÁCE, POŽÁRNÍ OCHRANA A OCHRANA ŽIVOTNÍHO PROSTŘEDÍ

- 9.1 Poskytovatel je povinen zajistit dodržování povinností vyplývajících z předpisů BOZP ze strany jeho zaměstnanců a/nebo ze strany zaměstnanců jeho poddodavatelů. V tomto směru je Poskytovatel povinen zajistit účast svých zaměstnanců a/nebo zaměstnanců poddodavatele na školení realizovaném ze strany Objednatele ve smyslu odst. 9.3 této Smlouvy.
- 9.2 Poskytovatel provedl vyhodnocení rizik ze svých činností a pracovní postupy doplní o opatření k eliminaci, resp. snížení těchto rizik. Poskytovatel prohlašuje, že se seznámil s pracovními podmínkami prostředí, ve kterém bude své činnosti provádět, posoudil možná rizika a bezpečnostní opatření promítnul do svých technologických postupů. Potenciální rizika Poskytovatele i Objednatele jsou uvedena v příloze č. 5, která je nedílnou součástí této Smlouvy.
- 9.3 Objednatel je povinen poskytnout zhotoviteli za účelem provádění díla dle této Smlouvy nezbytnou součinnost, která spočívá v zajištění:
- opatření povolení ke vstupu a vjezdu do areálů Objednatele ve prospěch zaměstnanců a dopravních prostředků zhotovitele či osob jednajících jménem a na účet zhotovitele v souvislosti s realizací díla;
  - proškolení zaměstnanců zhotovitele a příp. poddodavatelů v oblasti BOZP (bezpečnosti a ochrany zdraví při práci) a PO (požární ochrany) v českém jazyce. O proškolení bude sepsán „Zápis o základním nástupním školení a přezkoušení zaměstnanců a vedoucích zaměstnanců, cizích osob organizace, společnosti – externí firmy“ a „Zápis o školení zaměstnanců zhotovitele na příslušném pracovišti“. Zhotovitel je však povinen zajistit účast příslušných zaměstnanců, popř. zaměstnanců poddodavatelů při školení a v případě, že uvedení zaměstnanci budou cizinci, zajistí zhotovitel též, aby školení bylo pro uvedené zaměstnance zcela srozumitelné.
- 9.4 Zhotovitel je povinen dodržovat povinnosti označené jako „Povinnosti externího subjektu působícího v areálech společnosti Plzeňská teplárenská, a.s.“ a jako „PRAVIDLA vstupů, vjezdů a režim užívání společných komunikací v průmyslovém areálu ŠKODA v Plzni“, které jsou dostupné na stránkách objednatel [REDAKCE] v sekci „Ke stažení – Dokumenty“. Zhotovitel podpisem této Smlouvy potvrzuje, že se s těmito povinnostmi řádně seznámil.

## X. ZÁVĚREČNÁ USTANOVENÍ

- 9.1 Každá Smluvní strana je povinna nést veškeré náklady a výdaje, které jí vznikly v souvislosti s uzavřením dle této Smlouvy sama.
- 9.2 Tato Smlouva je vyhotovena v elektronické podobě.
- 9.3 Tato Smlouva nabývá platnosti 1. 7. 2026 a účinnosti dnem 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. Závazek mlčenlivosti a ochrany důvěrných informací zůstává v platnosti i po ukončení Smlouvy.
- 9.4 Tato Smlouva, jakož i práva a povinnosti vzniklé na základě této Smlouvy nebo v souvislosti s ní, se řídí právním řádem České republiky, zejména Občanským zákoníkem v platném znění.
- 9.5 Smluvní strany prohlašují, že pokud se kterékoliv ustanovení této Smlouvy nebo s ní související ujednání či jakákoli její část ukáže být neplatnými či se neplatnými stanou, neovlivní tato skutečnost platnost Smlouvy jako takové. V takovém případě se Smluvní strany zavazují nahradit neplatné ustanovení ustanovením platným, které se svým účelem nejvíce podobá neplatnému ustanovení.
- 9.6 Veškeré spory mezi Smluvními stranami vzniklé z této Smlouvy nebo v souvislosti s ní, budou řešeny, pokud možno, nejprve smírnou cestou - dohodou. Smluvní strany se dohodly, že nedojde-li k dohodě, místně příslušným soudem pro řešení případných sporů bude soud příslušný dle místa sídla Objednatele.
- 9.7 Tuto Smlouvu lze doplňovat nebo měnit pouze písemnými, číslovanými dodatky, podepsanými všemi Smluvními stranami.
- 9.8 Smluvní strany prohlašují, že tuto Smlouvu uzavřely ze své pravé, svobodné a vážně míněné vůle, nikoliv v tísní nebo za jinak nápadně nevýhodných podmínek. Dále Smluvní strany prohlašují, že si tuto Smlouvu před jejím uzavřením pročetly, jejímu obsahu zcela porozuměly a bezvýhradně s ním souhlasí a na důkaz toho k ní připojují své podpisy.
- 9.9 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.
- 9.10 Poskytovatel se zavazuje při plnění této smlouvy dodržovat veškeré požadavky na kybernetickou bezpečnost vyplývající ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti, v platném znění, a jeho prováděcích předpisů.
- 9.11 Podpisem této smlouvy Poskytovatel stvrzuje, že se seznámil s dokumentem Objednatele „Požadavky kybernetické bezpečnosti na významné dodavatele“, který tvoří Přílohu č. 5 této smlouvy. O případné aktualizaci bude informován Objednatelem e-mailem na kontaktní adresu v této Smlouvě.
- 9.12 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“).

- 9.13 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.
- 9.14 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.

**Přílohy:**

Příloha č. 1 - Seznam Oprávněných subjektů

Příloha č. 2 - Katalog služeb (rozsah plnění)

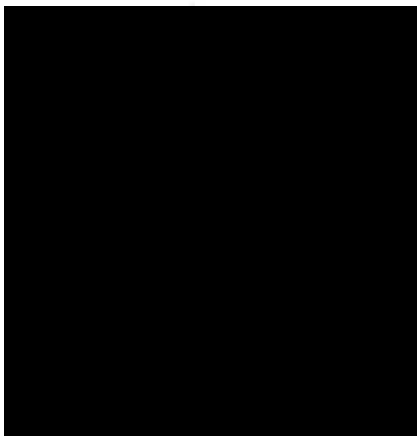
Příloha č. 3 - Tým / role a pověřené osoby

Příloha č. 4 - Hodnocení rizik

Příloha č. 5 - Požadavky kybernetické bezpečnosti na významné dodavatele

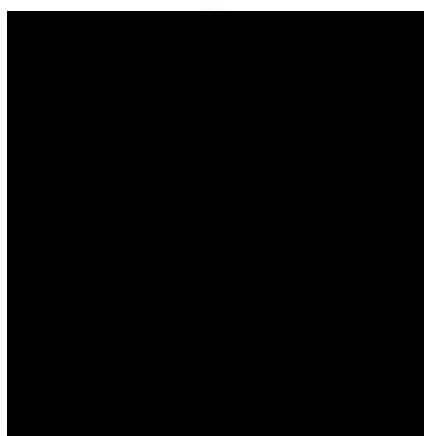
Za Poskytovatele:

V Opatovicích nad Labem dne

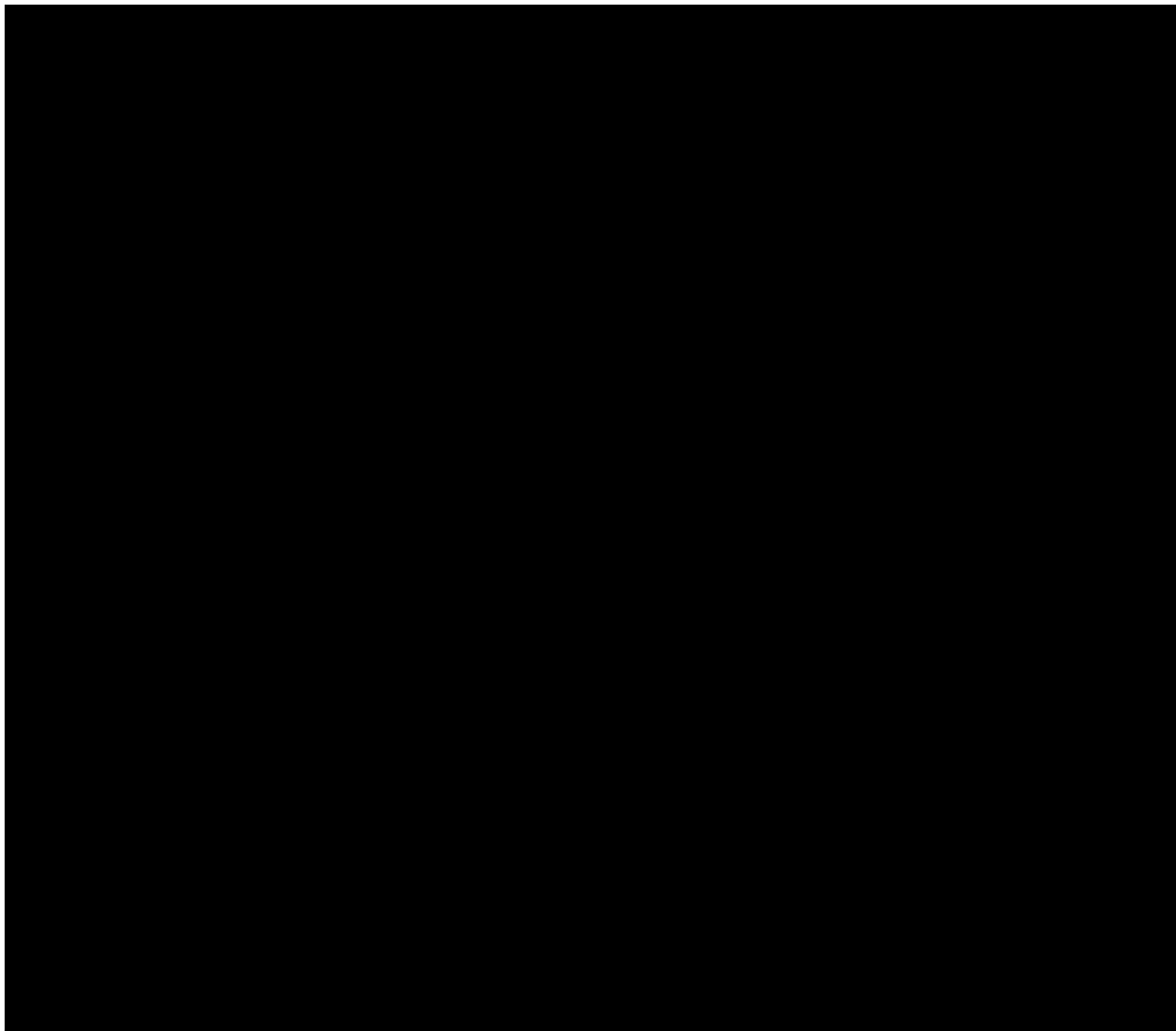


Za Objednatele:

V Plzni dne



**Příloha č. 1 – Seznam Oprávněných subjektů**



## **Příloha č. 2 – Katalog služeb (rozsah plnění)**

- Výkon role manažera kybernetické bezpečnosti / koordinace kybernetické bezpečnosti pro Objednatele a Oprávněné subjekty (řízení priorit, koordinace plnění opatření, eskalace, komunikace se stakeholdery);
- zajištění odborných činností architektů kybernetické bezpečnosti, zejména návrh a posuzování bezpečnostní architektury, stanovování bezpečnostních požadavků pro projekty a změny (security-by-design), posuzování bezpečnostních dopadů změn v ICT/OT prostředí;
- zajištění odborných činností specialisty kybernetické bezpečnosti, zejména metodická a realizační podpora zavádění bezpečnostních opatření, evidence a kontrola plnění dohodnutých úkolů a opatření, příprava podkladů a koordinace interních úkolů;
- metodická a koordinační podpora plnění povinností dle transpozice NIS2/nZKB (zákon č. 264/2025 Sb.) a souvisejících prováděcích předpisů, včetně průběžného vyhodnocování dopadů na Objednatele a Oprávněné subjekty dle režimu uvedeného v Příloze č. 1;
- návrh, údržba a rozvoj systému řízení kybernetické bezpečnosti (informační bezpečnosti) včetně nastavení rolí a odpovědností, evidence rozhodnutí a evidence výjimek;
- zpracování analýz rizik kybernetické bezpečnosti pro Objednatele a Oprávněné subjekty (sběr vstupů, identifikace hrozeb a zranitelností, návrh scénářů, vyhodnocení dopadů a pravděpodobnosti, návrh, prioritizace a průběžné vyhodnocování mitigací) ve spolupráci s relevantními vlastníky systémů a procesů na straně Objednatele;
- průběžná koordinace procesu řízení rizik kybernetické bezpečnosti včetně pravidelných přezkumů, eskalace zásadních rizik a reportingu vedení na základě dostupných podkladů Objednatele/Oprávněných subjektů;
- vedení a aktualizace obsahu registru rizik kybernetické bezpečnosti v nástroji určeném Objednatelem, přičemž Objednatel zajistí pořízení a provoz tohoto nástroje a zpřístupnění potřebných účtů/přístupů Poskytovateli;
- návrh, revize a aktualizace interních politik, směrnic, standardů a postupů kybernetické bezpečnosti (např. řízení přístupů, správa identit, správa aktiv, klasifikace informací, logování, zálohování, segmentace, správa zranitelností, řízení dodavatelů, řízení změn, řízení incidentů, business continuity a disaster recovery);
- průběžné hodnocení souladu (compliance) vůči požadavkům nZKB/NIS2 a interním standardům a návrh nápravných opatření;
- podpora při přípravě na audit/posouzení a při auditech a kontrolách (včetně koordinace podkladů, účasti na jednáních, připomínkování zjištění a návrhů nápravných opatření);
- koordinace a odborná podpora při řešení kybernetických bezpečnostních incidentů (triage, koordinace, návrh okamžitých opatření, evidence, komunikace se stakeholdery v dohodnutém rozsahu, post-incident review a návrh preventivních opatření);
- návrh a aktualizace procesů a provozních postupů pro řešení incidentů (včetně pravidel eskalace a kontaktní matice) a koordinace cvičení (table-top) dle dohody Smluvních stran;
- podpora při řízení dodavatelů z pohledu kybernetické bezpečnosti (bezpečnostní požadavky do smluv a objednávek, hodnocení rizik dodavatelů, požadavky na bezpečnostní opatření a reporting, účast na jednáních dle potřeby);
- návrh minimálních bezpečnostních požadavků (baseline) a doporučení pro technická a organizační opatření (např. IAM/MFA, PAM, SIEM/log management, EDR, patch management, hardening, segmentace, monitoring, zálohování, šifrování), včetně koordinace jejich zavádění na úrovni požadavků a dohledu nad plněním;
- pravidelný reporting vedení v dohodnuté periodicitě obsahující zejména stav plnění opatření, otevřená rizika, incidenty, výjimky, plán aktivit a priority;
- koordinace a facilitace pravidelných jednání ke kybernetické bezpečnosti (operativní a řídicí), včetně přípravy podkladů, zápisů a akčních bodů;

- konzultační a metodická podpora pro klíčové role a týmy Objednatele/Oprávněných subjektů (IT, OT, compliance, právní, nákup, provoz) v otázkách kybernetické bezpečnosti;
- podpora v oblasti zvyšování povědomí (awareness) – návrh obsahu a realizace cílených školení pro management a vybrané role dle dohody Smluvních stran.

#### **Vymezení odpovědností k nástroji pro rizika**

- Objednatel zajistí pořízení, licencování a provoz nástroje pro evidenci registru rizik (včetně správy přístupů a dostupnosti nástroje). Poskytovatel nenes odpovědnost za dodávku ani provoz tohoto nástroje; v případě jeho dočasné nedostupnosti může Poskytovatel po dohodě poskytovat výstupy v náhradní formě.

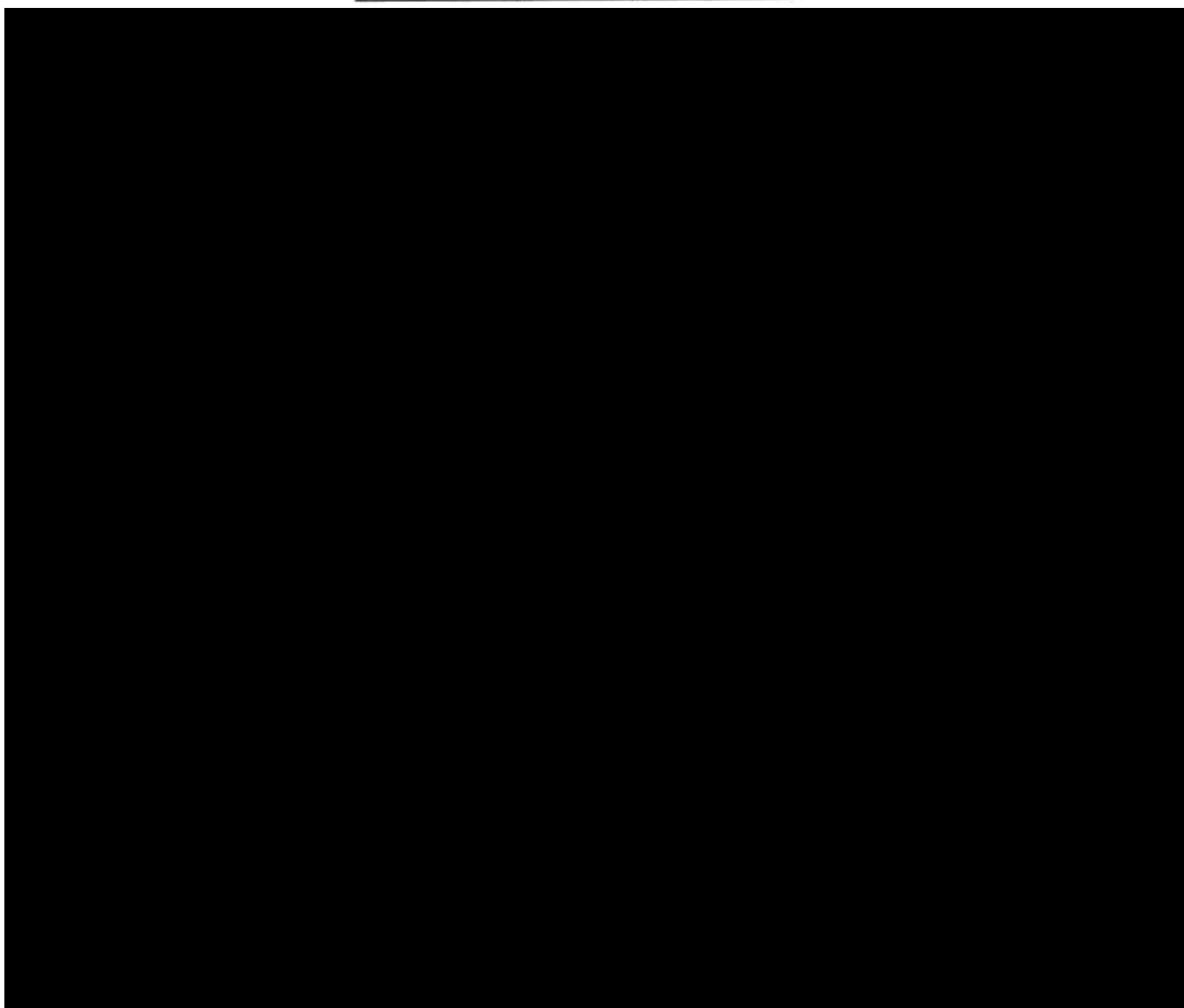
#### **Výslovně mimo rozsah (není-li sjednáno samostatně)**

- Nepřetržitý dohled 24/7 (SOC) a kontinuální monitoring;
- penetrační testy, forenzní analýzy, technické skeny/testování a specializované laboratorní analýzy;
- provozní správa ICT/OT systémů Objednatele (administrace serverů, sítí, koncových stanic, aplikací);
- dodávky, licencování a provoz bezpečnostních nástrojů (SIEM, EDR, PAM apod.), včetně jejich implementace jako projektové dodávky.

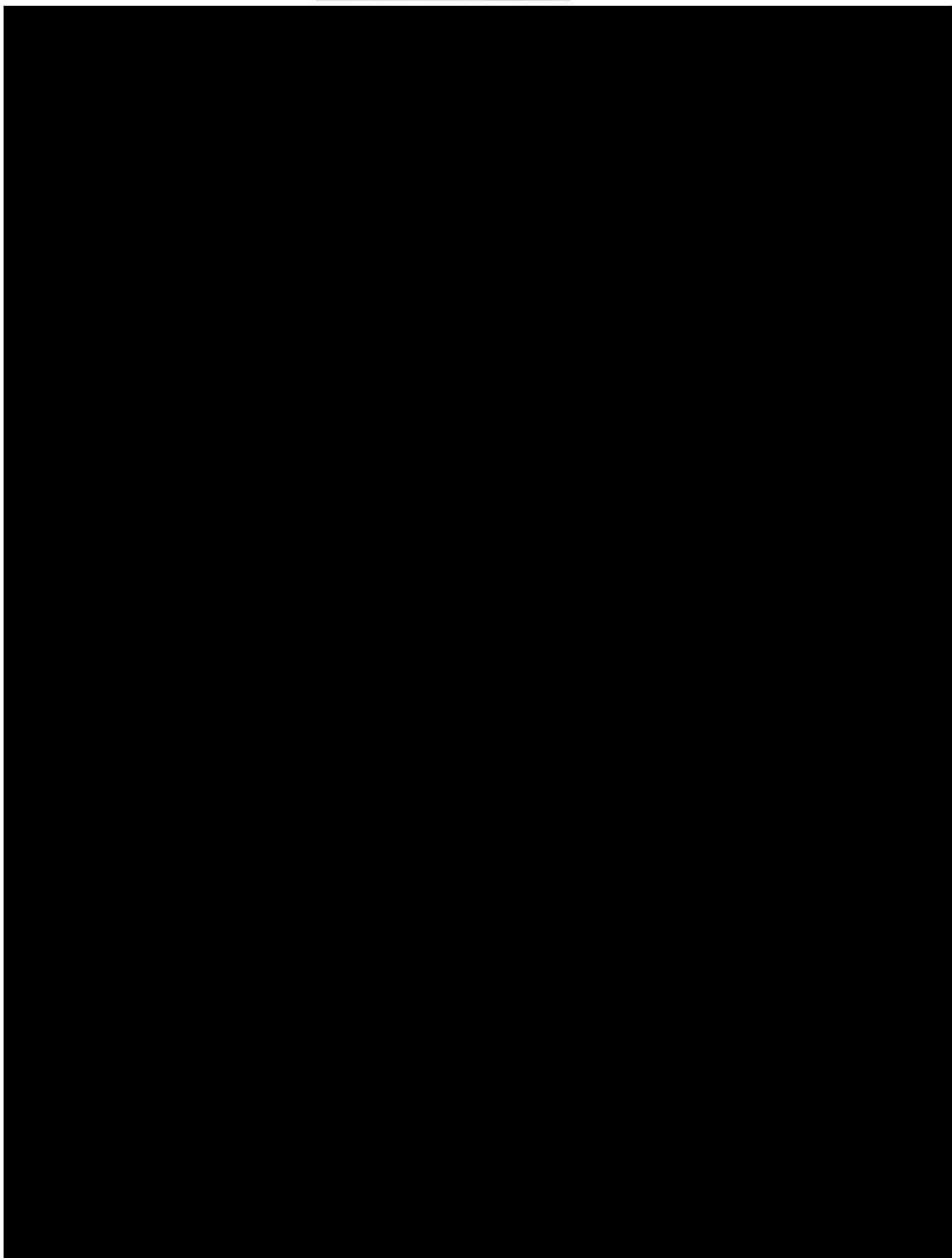
#### **Změny rozsahu**

- Poskytování služeb mimo výše uvedený katalog nebo dlouhodobé navýšení kapacity bude realizováno pouze na základě písemně schválené změny (změnový list/dodatek) dle pravidel sjednaných ve Smlouvě.

**Příloha č. 3 – Tým / role a pověřené osoby**



**Příloha č. 4 – Hodnocení rizik**



## **Příloha č. 5 – Požadavky kybernetické bezpečnosti pro významné dodavatele**

### **Obsah:**

Obsah:.....	<b>Chyba! Záložka není definována.</b>
1 Základní pojmy a zkratky.....	<b>Chyba! Záložka není definována.</b>
2 Úvodní ustanovení.....	<b>Chyba! Záložka není definována.</b>
3 Pravidla pro Zhotovitele.....	<b>Chyba! Záložka není definována.</b>
3.1 Fyzická bezpečnost – pohyb v areálu Objednatele.....	<b>Chyba! Záložka není definována.</b>
3.2 Řízení do přístupu do sítě.....	<b>Chyba! Záložka není definována.</b>
3.3 Politika hesel.....	<b>Chyba! Záložka není definována.</b>
3.4 Požadavky na zařízení připojovaná do sítě Objednatele ...	<b>Chyba! Záložka není definována.</b>
3.5 Instalace SW.....	<b>Chyba! Záložka není definována.</b>
3.6 Výměnná paměťová média.....	<b>Chyba! Záložka není definována.</b>
3.7 Zakázané činnosti.....	<b>Chyba! Záložka není definována.</b>
3.8 Hlášení kybernetických bezpečnostních incidentů.....	<b>Chyba! Záložka není definována.</b>
3.9 Monitoring činností.....	<b>Chyba! Záložka není definována.</b>
3.10 Klasifikace a pravidla nakládání s informacemi.....	<b>Chyba! Záložka není definována.</b>

## 1. ZÁKLADNÍ POJMY A ZKRATKY

<b>Smlouva</b>	Smlouva o dílo/Kupní smlouva/Rámcová smlouva o poskytování služeb jejíž přílohou je tento dokument.
<b>System</b>	Služby/dodávky specifikované v Předmětu díla Smlouvy a jejích přílohách.
<b>Objednatel</b>	Plzeňská teplárenská, a.s.
<b>Informační bezpečnost</b>	Ochrana informací a informačních systémů před neoprávněným přístupem, užíváním, odhalením, rušením, změnou, inspekcí, záznamem nebo zničením s cílem zabezpečit jejich důvěrnost, integritu a dostupnost.
<b>Kybernetická bezpečnost</b>	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.
<b>Prostředky Objednatele</b>	Hmotné i nehmotné věci ve vlastnictví nebo nájmu Objednatele, které jsou nezbytné k plnění předmětu Smlouvy.
<b>Prostředí Objednatele</b>	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.
<b>Prostředky Zhotovitele</b>	Hmotné i nehmotné věci ve vlastnictví nebo nájmu Zhotovitele, které jsou nezbytné k plnění předmětu Smlouvy.
<b>Prostředí Zhotovitele</b>	Fyzický perimetr určený ohraničením fyzického prostoru v nájmu nebo majetku Zhotovitele anebo logický perimetr definovaný hraničními prvky informačního/komunikačního systému ve správě nebo majetku Zhotovitele.
<b>VoKB</b>	Vyhláška č. 409/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
<b>ZoKB</b>	Zákon č. 264/2025 Sb., o kybernetické bezpečnosti
<b>Osobní údaje</b>	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, psychologické, ekonomické, kulturní nebo společenské identity této fyzické osoby).
<b>Zpracování osobních údajů</b>	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

Plzeňská teplárenská, a.s. (dále jen „PLTEP“) je subjektem spadajícím pod zákon č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „ZoKB“). Z tohoto důvodu jsou na dodavatele aplikovány níže uvedená pravidla.

## 3. PRAVIDLA PRO ZHOTOVITELE

Pracovník Zhotovitele prohlašuje, že byl prokazatelně seznámen s podmínkami a náležitostmi Smlouvy, na základě, které bude provádět pracovní činnost pro PLTEP. Tyto podmínky se zavazuje dodržovat a dále je povinen dodržovat níže uvedená pravidla, která se vztahují na práci v prostředí Objednatele:

- s prostředky Zhotovitele;
- s prostředky Objednatele;
- mimo prostředí Objednatele.

Při veškeré činnosti musí pracovník Zhotovitele dodržovat předepsané a doporučené pracovní postupy a metody, aby nedošlo k narušení kybernetické bezpečnosti a bezpečnosti informací.

### **3.1 Fyzická bezpečnost – pohyb v areálu Objednatele**

V rámci své činnosti má pracovník Zhotovitele oprávnění vstupovat pouze do prostor, které jsou nezbytné pro vykonávání jeho činnosti.

Zhotovitel je povinen informovat garanta Smlouvy Objednatele e-mailem nejméně 24 hodin před příjezdem do areálu Objednatele. V případě nedodržení časové lhůty pro informování garanta Smlouvy Objednatele o příjezdu Zhotovitele nemusí být Zhotovitel vpuštěn do areálu Objednatele.

### **3.2 Řízení do přístupu do sítě**

Přidělení oprávnění přístupu do prostředí Objednatele pracovníkovi Zhotovitele se řídí principem nezbytného minima a není nárokové.

Pracovník Zhotovitele má zakázáno sdílet autentizační prostředky pro přístup do prostředí Objednatele s jinými osobami. Případná výjimka musí být schválena odpovědnou osobou Objednatele a musí být na straně Zhotovitele evidována. Za sdílené autentizační prostředky odpovídá žádající osoba o výjimku na straně Zhotovitele.

Přístupová oprávnění budou využívána výhradně k účelům splnění předmětu Smlouvy.

Pokud má pracovník Zhotovitele v rámci plnění Díla právo používat privilegovaná oprávnění, musí je využívat jen v přiměřené míře a jen pro dobu nezbytně nutnou pro vykonání činností v souladu s plněním předmětu Smlouvy. Privilegovaná oprávnění nesmí být využívána pro běžnou práci.

### **3.3 Politika hesel**

Pracovník Zhotovitele musí dodržovat předepsanou politiku hesel:

- délka hesla min. 12 znaků (uživatel) / 17 znaků (administrátor)
- kombinace malé/velké písmeno, číslice, speciální znak (alespoň 3 z uvedených)
- heslo NESMÍ obsahovat:
  - nejčastěji používaná hesla,
  - přihlašovací jméno, e-mail, název systému a obdobně
  - opakované či sekvenční sady (třeba zzzz nebo abc456)
  - jména a/nebo data narození uživatele, jeho přátel či příbuzných;
  - kombinace obsahující aktuální rok, měsíc nebo roční období (např. Summer2018);

Hesla nesmí poznamenána v čitelné formě ať už písemně nebo elektronicky (soubory, mail).

Prozrazená hesla musí být okamžitě změněna a jakékoli incidenty s vyzrazením nebo zneužitím přihlašovacích údajů musí být neprodleně ohlášeny příslušnému pracovníkovi Objednatele.

Pracovník Zhotovitele, kterému je uživatelský účet přidělen, je plně odpovědný za veškeré aktivity provedené tímto účtem v počítačové síti.

Výjimka z politiky hesel musí být schválena Architektem KB Objednatele.

### **3.4 Požadavky na zařízení připojovaná do sítě Objednatele**

Připojovat do prostředí Objednatele (ať místně do LAN nebo vzdáleně přes VPN přístup) lze pouze výslovně schválená zařízení (viz. Příloha č.1 PIKYB – Žádost o zřízení přístupu do sítě PLTEP), která musí splňovat:

- Veškerý nainstalovaný SW je legální a splňuje licenční podmínky výrobce.
- Operační systém s platnou servisní podporou výrobce (vydávání bezpečnostních update).
- Funkční a pravidelně prováděné automatické aktualizace bezpečnostních záplat veškerého SW

(OS, Office, JAVA, SQL, apod...).

- Funkční a pravidelně aktualizovanou antivirovou ochranou se zapnutým rezidentním štítem.
- Nastavenou automatickou antivirovou kontrolu po vložení výměnných médií (USB, CD/DVD, apod).
- Funkční personální firewall s nastavením pouze nezbytných pravidel.
- Musí být připojeno do sítě Objednatele na místě, které definuje Objednatel.

Pokud je zařízení pracovníka Zhotovitele připojeno do vnitřní sítě Objednatele, NESMÍ být současně připojeno k internetu (přes WiFi, LTE, mobilní Hotspot apod...).

### **3.5 Instalace SW**

Instalovat SW do prostředí Objednatele je možné pouze po předchozím schválení instalačních postupů ze strany Objednatele.

### **3.6 Výměnná paměťová média**

V prostředí Objednatele je povoleno používat pouze registrovaná výměnná média (USB flash, externí HDD), která jsou evidovaná. Na paměťovém médiu mohou být uloženy pouze informace a data bezprostředně související s předmětem Díla, které Zhotovitel vykonává pro Objednatele. Zhotovitel odpovídá za bezpečnost výměnných paměťových médií a jejich pravidelnou kontrolu po celou dobu projektu. O využívání výměnných médií souvisejících s předmětem Díla musí Zhotovitel vést evidenci.

Data mohou na paměťovém médiu uložena pouze po nezbytně nutnou dobu (např. přenos dat mezi různými systémy), Výměnné paměťové médium nesmí být v žádném případě používána pro dlouhodobé zálohování dat a informací.

Na výměnných paměťových médiích nesmí být ukládány informace kategorie VYSOKÉ a KRITICKÉ.

### **3.7 Zakázané činnosti**

Pracovníkům Zhotovitele je zakázáno:

- bez předchozí domluvy s odpovědným pracovníkem PLTEP provádět jakékoliv činnosti na prvcích komunikační sítě OBJEDNATELE (switche, kabeláže);
- ukládat nebo sdílet data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno OBJEDNATELE;
- stahoval, sdílet/šířit, ukládat ani instalovat datové a spustitelné soubory v rozporu s licenčními podmínkami nebo s ochranou duševního vlastnictví;
- navštěvovat internetové stránky s eticky nevhodným obsahem;
- šířit spamu a obdobný nevyžádaný obsah;
- pokoušet se o jakýkoliv neautorizovaný přístup.

V prostředí Objednatele je dále zakázáno instalovat nebo používat tyto typy nástrojů, pokud nejsou součástí předmětu plnění:

- Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.
- Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.
- Analyzátor zranitelností (scanner zranitelností) – softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT/ICS, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.
- Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejítí schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT/ICS.
- Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí Objednatele.
- Obdobné rizikové nástroje, který mají za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

### **3.8 Hlášení kybernetických bezpečnostních incidentů**

Zhotovitel musí bez prodlení hlásit odpovědným pracovníkům Objednatele všechna podezření na kybernetické bezpečnostní události a incidenty a spolupracovat na jejich řešení poskytnutím nezbytné součinnosti a informací/dat.

**Kybernetickou bezpečnostní událostí** je událost, která ***může způsobit narušení*** bezpečnosti informací v informačních systémech, nebo narušení bezpečnosti služeb, anebo bezpečnosti a integrity sítí elektronických komunikací (tedy KB událost, která má potenciál být KB incidentem).

**Kybernetickým bezpečnostním incidentem** je ***narušení*** bezpečnosti informací v informačních systémech, nebo narušení bezpečnosti služeb, anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události, tedy v zásadě každé narušení zajištění důvěrnosti, integrity a dostupnosti informací a dat a narušení dostupnosti nebo interoperability služeb a integrity sítí (tedy KB událost, u které bylo ověřeno, že jde o reálné/skutečné narušení).

### **3.9 Monitoring činností**

Přístup a aktivity pracovníků Zhotovitele k aktivům a infrastruktuře Objednatele jsou nepřetržitě zaznamenávány, monitorovány a vyhodnocovány.

Pracovník Zhotovitele bere na vědomí, že v případě podezření na závadné nebo nestandardní chování může být příslušný účet zablokován a případně mohou být aktivovány postupy pro zvládnání bezpečnostních incidentů.

### **3.10 Klasifikace a pravidla nakládání s informacemi**

Pracovník musí dodržovat pravidla nakládání s informacemi dle jejich klasifikace (příloha č. 2 – Pravidla ochrany kybernetických aktiv). Pokud není uvedeno jinak, veškeré informace obdržené od Objednatele se pokládají za **INTERNÍ**. V návaznosti na klasifikaci informací se musí pracovník Zhotovitele řídit příslušným způsobem mazání a likvidace dat a informací dle jejich klasifikace (Příloha č. 3 PIKYB – Způsob mazání a likvidace dat a informací).

**PIKYB – Příloha č. 1 – Žádost o zřízení přístupu do sítě Plzeňská teplárenská, a.s.**

**Žádost o zřízení přístupu do sítě Plzeňská teplárenská, a.s.**

<b>Základní informace o objednavateli</b>	
Název společnosti:	
Jméno a příjmení žadatele <sup>1</sup> :	
Kontaktní e-mail odpovědné osoby:	
Telefon odpovědné osoby:	
Důvod pro udělení přístupu:	
Seznam uživatelů, kteří budou využívat přístupu (jméno, email, mobilní telefon):	
Datum zahájení přístupu:	Datum ukončení přístupu:
<b>Odpovědná osoba (garant) za Plzeňskou teplárenskou, a.s.</b>	
Jméno a příjmení:	
Funkce:	
Osobní číslo:	
Telefon:	
<b>Požadavky na přístup</b>	
Druh (popsat) požadovaného přístupu <sup>2</sup> :	
Aplikace/Server/PC <sup>3</sup> :	
Zařízení, která budou použita pro přístup (MAC adresa) <sup>4</sup> :	
Poznámky k upřesnění požadavku <sup>5</sup> :	

V rámci zřízeného připojení je zakázáno sdílet připojení nebo informace o připojení s osobami, které nejsou uvedeny v seznamu (formulář – Žádost o zřízení přístupu do sítě Plzeňská teplárenská, a.s.).

Připojovat se do sítě Plzeňské teplárenské, a.s. je možné pouze se zařízením, které je pravidelně aktualizováno a které používá aktivně antivirovou ochranu s aktualizovanou virovou databází. Součástí odevzdané žádosti bude i čestné prohlášení, že zařízení tyto požadavky splňuje.

Jakékoliv připojování USB zařízení do zařízení Plzeňské teplárenské, a.s. je zakázáno. Pokud je potřeba přenést data do zařízení společnosti Plzeňská teplárenská, a.s. je povoleno jen po kontrole administrátorem a vždy jen na zařízeních (USB flash disk, externí disk atd.) v majetku Plzeňská teplárenská, a.s.

Pro přenos dat v rámci sítě je potřeba využít k tomuto určené sdílené síťové uložení.

Společnost Plzeňská teplárenská, a.s. si z důvodu zajištění bezpečnosti své sítě vyhrazuje právo na namátkovou kontrolu zařízení žadatele, které se budou připojovat do její sítě. Pokud budou shledána závažná pochybení ze strany žadatele, bude mu přístup do sítě Plzeňské teplárenské, a.s. zakázán.

Podpisem této žádosti žadatel stvrzuje, že bere na vědomí všechny podmínky uvedené v této žádosti a souhlasí s jejich dodržování.

Datum a podpis žadatele	Za Plzeňskou teplárenskou, a.s. (Garant)

**PIKYB – Příloha č. 2 – Pravidla ochrany kybernetických aktiv**

Požadavky na rozlišování, manipulaci, přípustný způsob použití, resp. požadavky na ochranu kybernetických aktiv uvádí následující tabulka, a to v závislosti na úrovni aktiv – dle hodnocení aktiv z hlediska Důvěrnosti, Dostupnosti a Integrity.

POŽADAVKY NA OCHRANU AKTIVA				
ÚROVEŇ / HODNOCENÍ AKTIVA				
	1 - NÍZKÁ	2 - STŘEDNÍ	3 - VYSOKÁ	4 - KRITICKÁ
<b>Označení</b>	Není vyžadováno. Dokumenty lze označit textem „ <b>Veřejné</b> “ V případě sdílení nebo výměny dle TPL možno označit TLP:WHITE	Dokumenty označit textem „ <b>Interní</b> “. V případě sdílení nebo výměny dle TPL možno označit TLP:GREEN nebo TLP:AMBER	Dokumenty označit textem „ <b>Citlivé</b> “ nebo „ <b>Důvěrné</b> “. V případě sdílení nebo výměny dle TPL možno označit TLP:AMBER	Dokumenty označit textem „ <b>Vysoce citlivé</b> “ nebo „ <b>Tajné</b> “. V případě sdílení nebo výměny dle TPL možno označit TLP:RED nebo TLP:AMBER
<b>Přístup</b>	Není vyžadována žádná ochrana. Pro veřejné použití.	Řízení přístupu. Pro interní použití.	Řízení přístupu, omezení přístupových práv pro zápis. Jen pro určené příjemce / uživatele (dle pracovního zařazení).	Řízení přístupu a pokusů o přístup, omezení přístupových práv pro zápis. Jen pro úzký a písemně definovaný okruh příjemců / uživatelů.
<b>Uložení</b>	Není vyžadována žádná ochrana.	Definované úložiště	Definované úložiště, může být šifrováno	Definované úložiště, které je šifrováno.
<b>Kopie</b>	Není vyžadována žádná ochrana.	Není vyžadována žádná ochrana.	Informovat Garanta.	Písemné svolení Garanta.
<b>Změny</b>	Evidence verzí.	Evidence verzí.	Sledování historie provedených změn včetně identity osoby provádějící změnu.	Sledování historie provedených změn včetně identity osoby provádějící změnu. Digitální podpis prováděných změn.

POŽADAVKY NA OCHRANU AKTIVA				
	ÚROVEŇ / HODNOCENÍ AKTIVA			
	1 - NÍZKÁ	2 - STŘEDNÍ	3 - VYSOKÁ	4 - KRITICKÁ
<b>Pošta</b>	Není vyžadována žádná ochrana.	Není vyžadována žádná ochrana. Pro interní nebo smluvní příjemce.	V zalepené obálce. Jen pro určené příjemce.	V zalepené obálce. Jen pro úzký a písemně definovaný okruh příjemců.
<b>e-mail</b>	Není vyžadována žádná ochrana.	Není vyžadována žádná ochrana. Pro interní nebo smluvní příjemce.	Kryptografické zabezpečení. Jen pro určené příjemce.	Kryptografické zabezpečení. Jen pro úzký a definovaný okruh příjemců.
<b>LAN / WAN</b>	Není vyžadována žádná ochrana.	Není vyžadována žádná ochrana.	Doporučené kryptografické zabezpečení přenosu dat komunikační sítí mimo uzavřené řídicí systémy.	Kryptografické zabezpečení přenosu dat komunikační sítí.
<b>Internet</b>	Řízení přístupu, omezení přístupových práv pro zápis.	Řízení přístupu, omezení přístupových práv pro zápis.	Kryptografické zabezpečení.	Kryptografické zabezpečení.
<b>Manipulace</b>	Se svolením Garanta.	Se svolením Garanta.	Se svolením Garanta dle odsouhlaseného postupu.	Se svolením Garanta dle písemně odsouhlaseného postupu.
<b>Zálohy / Dostupnost</b>	Zálohování podle potřeby.	Pravidelné zálohování. Testování plánů obnovy.	Cold Backup Záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.	Warm / Hot Backup Běžící záložní systémy, obnova poskytování služeb je krátkodobá a automatizovaná.

**PIKYB – Příloha č. 3 – Způsoby mazání a likvidace dat a informací**

Způsoby spolehlivého mazání nebo ničení technických nosičů dat, informací, provozních údajů a jejich kopií uvádí následující tabulka, a to v závislosti na úrovni aktiv – dle hodnocení aktiv z hlediska Důvěrnosti, Dostupnosti a Integrity.

Lze použít náročnější a spolehlivější způsob mazání a likvidace, než odpovídá dané úrovni / hodnocení aktiva, minimálně však způsob odpovídající dané úrovni.

<b>Způsoby spolehlivého mazání nebo ničení technických nosičů dat, informací, provozních údajů a jejich kopií</b>				
<b>Úroveň / Hodnocení aktiva</b>				
	<b>1 – Nízká / Veřejné</b>	<b>2 – Střední / Interní</b>	<b>3 – Vysoká / důvěrná</b>	<b>4 – Kritická / tajná</b>
Informace na lidsky čitelném nosiči (tištěné dokumenty, poznámky a podobně)	Odstranění: Vyhození do odpadu.	Přepsání: Začernění.	Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje, spálením nebo rozložením.	Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje s podélným i příčným řezem, spálením nebo rozložením.
Mobilní zařízení (mobilní telefony, tablety)	Odstranění: Vymazání informací, reset zařízení do továrního nastavení.	Odstranění: Vymazání informací, reset zařízení do továrního nastavení.	Přepsání: Pro zařízení s šifrovaným úložištěm – odstranění informací a reset do továrního nastavení.	Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací.
Síťová zařízení (router, switch, modem a podobně)	Odstranění: Vymazání informací, reset do továrního nastavení.	Odstranění: Vymazání informací, reset do továrního nastavení.	Přepsání: Odstranění a zahlcení umělými událostmi (umělý síťový provoz a podobně.).	Přepsání: Odstranění a zahlcení umělými událostmi (umělý síťový provoz a podobně.).
Kancelářské vybavení (scanery, tiskárny, fax)	Odstranění: Vymazání informací.	Odstranění: Vymazání informací, reset do továrního nastavení.	Přepsání: Odstranění a zahlcení umělými událostmi (umělý síťový provoz, testovací tiskové úlohy a podobně.).	Přepsání: Odstranění a zahlcení umělými událostmi (umělý síťový provoz, testovací tiskové úlohy a podobně.).
Magnetická média (magnetické pásky, disky, HDD [Hard Disk Drive])	Odstranění: Smazání dat na úrovni souborového systému.	Přepsání: Přepsání dat. V případě šifrovaného média je alternativou bezpečná likvidace kryptografických klíčů	Přepsání: Odstranění a vícenásobné přepsání umělými daty. V případě šifrovaného média je alternativou bezpečná likvidace kryptografických klíčů	Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací.

Způsob spolehlivého mazání nebo ničení technických nosičů dat, informací, provozních údajů a jejich kopií				
	Úroveň / Hodnocení aktiva			
	1 – Nízká / Veřejné	2 – Střední / Interní	3 – Vysoká / důvěrná	4 – Kritická / tajná
Optická média (CD, DVD, HD-DVD, BLU-RAY)	Fyzická likvidace.	Fyzická likvidace.	Fyzická likvidace.	Fyzická likvidace.
Elektronická média (flash paměti)	Odstranění: Smazání dat na úrovni souborového systému.	Přepsání: Přepsání dat. V případě šifrovaného média je alternativou bezpečná likvidace kryptografických klíčů	Fyzická likvidace.	Fyzická likvidace.
Outsourcing a cloud Přípustný způsob likvidace dat by měl být stanoven smluvním ujednáním.	Odstranění: Odstranění všech souborů včetně předchozích verzí.	Odstranění: Odstranění všech souborů včetně předchozích verzí.	Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů.	Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů uložených v certifikovaném hardware security modulu (HSM) řízená zákazníkem (například podle standardu FIPS 140-2 Level 2). Při ukončení služby bude zlikvidován vrchní přístupový klíč a data jsou přepsána.