PLZEŇSKÁ TEPLÁRENSKÁ
Více než energie



Smlouva o poskytování služby kybernetické bezpečnosti

uzavřená mezi společnostmi Plzeňská teplárenská, a.s. a Plzeňská teplárenská Energetické služby, s.r.o.

číslo smlouvy: O2026/0117

Plzeňská teplárenská, a. s., Doubravecká 2760/1, 301 00 Plzeň
tel.: +420 377 180 111, fax: +420 377 235 845
e-mail: inbox@plzenskateplarenska.cz, 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
BUREAU VERITAS

Plzeňská teplárenská, a.s.
se sídlem v Plzni, Doubravecká 2760/1, Východní Předměstí, PSČ 301 00
zapsána v OR vedeném Krajským soudem v Plzni oddíl B, vložka 392
zastoupena na základě plné moci a pověření ze dne 21. 5. 2025 [redacted]
IČ: 49790480
DIČ: CZ49790480
bankovní spojení: [redacted]

(dále jen „**Poskytovatel**“)

a

Plzeňská teplárenská Energetické služby, s.r.o.
se sídlem v Plzni, Doubravecká 2760/1, Východní Předměstí, PSČ 301 00
zapsána v OR vedeném Krajským soudem v Plzni oddíl C, vložka 19900
zastoupená Ing. Jiřím Králem a Jakubem Vojtou, BBS, jednateli společnosti
IČ: 27980502
DIČ: CZ27980502
bankovní spojení: [redacted], č. ú.: [redacted]

(dále jen „**Objednatel**“)

(Poskytovatel a Objednatel jsou níže společně též nazýváni jako „**Smluvní strany**“ nebo jednotlivě jako „**Smluvní strana**“)

sjednávají jako Smluvní strany dle ust. § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku v platném znění níže uvedenou Smlouvu o poskytování služeb zajištění kybernetické bezpečnosti (dále jen „**Smlouva**“) v tomto znění:

I.
Předmět Smlouvy

1.1 Předmětem Smlouvy je závazek Poskytovatele podle podmínek sjednaných ve Smlouvě poskytovat Objednateli prostřednictvím subdodavatele službu kybernetické bezpečnosti spočívající zejména v zajištění odborných činností a podpory nezbytné k plnění povinností, které na Objednatele 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 poskytované služby kybernetické bezpečnosti je vymezen v **Příloze č. 1** Smlouvy (dále jen „**Služby**“). V případě rozporu mezi ustanoveními Smlouvy a Přílohou č. 1 Smlouvy má přednost vymezení uvedené v Příloze č. 1 Smlouvy.

1.2 Poskytovatel výslovně prohlašuje, že poskytované plnění dle Smlouvy prostřednictvím subdodavatele 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 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 prostřednictvím subdodavatele 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 Smlouvy.

2.4 Poskytovatel se zavazuje zajistit, že pověřená osoba subdodavatele bude Služby dle Smlouvy poskytovat osobně v sídle Objednatele nebo prostřednictvím prostředků komunikace na dálku. Fyzická přítomnost pověřené osoby subdodavatele 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 subdodavatele, 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 pověřené osobě subdodavatele veškerou jemu dostupnou dokumentaci a informace nezbytné k řádnému plnění 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 pověřené osobě subdodavatele 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 pověřené osobě subdodavatele součinnost nezbytnou k řádnému plnění jeho povinností dle Smlouvy. Pověřená osoba subdodavatele 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 a subdodavatele pro plnění předmětu Smlouvy definovaných v **Příloze č. 2** Smlouvy. Poskytovatel a subdodavatel jsou oprávněni jednostranně změnit pověřenou osobu uvedenou v Příloze č. 2 Smlouvy, a to písemným oznámením doručeným Objednateli.

2.7 Smluvní strany se dohodly, že na plnění předmětu Smlouvy se bude podílet třetí strana, se kterou má Poskytovatel uzavřenou smlouvu. Plní-li předmět Smlouvy třetí osoba, odpovídá za její plnění Poskytovatel, jako by plnil sám.

2.8. Poskytovatel se zavazuje aktualizovat rozsah a obsah poskytované služby kybernetické bezpečnosti, který je vymezen v **Příloze č. 1** Smlouvy, tak aby byly Smlouvou plněny všechny podmínky dle zákona č. 264/2025 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, souvisejících prováděcích právních předpisů a metodických či závazných opatření vydávaných příslušnými orgány veřejné moci, zejména Národním úřadem pro kybernetickou a informační bezpečnost.

III.
Cena a platební podmínky

3.1 Smluvní strany se dohodly, že měsíční paušální cena za poskytování Služeb podle Smlouvy činí [redacted] **Kč** (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 Platby budou prováděny měsíčně na základě faktur vystavených Poskytovatelem do 15. dne kalendářního měsíce následujícího po kalendářním měsíci, za nějž je fakturováno. Vystavený daňový doklad bude zaslán elektronicky na e-mailovou adresu Objednatele: [redacted]

3.3 Faktura (daňový doklad) vystavená Poskytovatelem musí kromě náležitostí požadovaných obecně závaznými právními předpisy obsahovat také číslo smlouvy popř. č. objednávky, údaj o době splatnosti faktury uvedený v souladu se Smlouvou a dále vyčíslení zvlášť ceny Služeb bez DPH, zvlášť DPH a cenu Služeb včetně DPH.

3.4 Smluvní strany se dohodly na lhůtě splatnosti faktury v délce čtrnácti (14) kalendářních dnů ode dne vystavení faktury Objednateli. Cena za poskytnuté Služby se považuje za uhrazenou okamžikem připsání fakturované ceny za poskytnuté Služby na bankovní účet Poskytovatele.

IV.
Platnost Smlouvy a odstoupení od Smlouvy

4.1 Smlouva se uzavírá **na dobu 3 let**. Kterákoli Smluvní strana je oprávněna vypovědět 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 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 prostřednictvím subdodavatele odpovídá Objednateli za škody, které vyplývají nebo jsou výsledkem porušení právních předpisů, norem či smluvních povinností subdodavatele v souvislosti s výkonem činností dle 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 Smluvní strany. Nedodržení závazků dle článku 2.5 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 Smluvní strany a brání jí ve splnění její povinnosti, jestliže nelze rozumně předpokládat, že by povinná Smluvní 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 Smluvní 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 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 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 Smlouvy všechny osoby (včetně subdodavatele uvedeného v Příloze č. 2 Smlouvy), které se budou podílet na poskytování plnění Objednateli dle Smlouvy.

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

VIII.
Ostatní ujednání

8.1 Smluvní strany jsou povinny bez zbytečného odkladu oznámit druhé Smluvní straně změnu údajů v záhlaví Smlouvy.

8.2 Poskytovatel není bez předchozího písemného souhlasu Objednatele oprávněn postoupit práva a povinnosti ze Smlouvy na třetí osobu. Objednatel není bez předchozího písemného souhlasu Poskytovatele oprávněn postoupit práva a povinnosti ze Smlouvy na třetí osobu.

8.3 Každá ze Smluvních stran je povinna dokumenty související s poskytováním Služeb dle 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 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 subdodavatele. V tomto směru je Poskytovatel povinen zajistit účast svých zaměstnanců a/nebo zaměstnanců subdodavatele na školení realizovaném ze strany Objednatele ve smyslu odst. 9.3 Smlouvy.

9.2 Poskytovatel prohlašuje, že jeho subdodavatel provedl vyhodnocení rizik ze svých činností a pracovní postupy doplní o opatření k eliminaci, resp. snížení těchto rizik. Poskytovatel zajistí, aby se subdodavatel seznámil s pracovními podmínkami prostředí, ve kterém bude své činnosti provádět, posoudil možná rizika a bezpečnostní opatření promítnul do svých technologických postupů. Potenciální rizika subdodavatele jsou uvedena v **Příloze č. 3**, která je nedílnou součástí Smlouvy.

9.3 Objednatel je povinen poskytnout subdodavateli za účelem poskytování Služeb dle Smlouvy nezbytnou součinnost, která spočívá v zajištění:

a) opatření povolení ke vstupu a vjezdu do areálů Objednatele ve prospěch zaměstnanců a dopravních prostředků subdodavatele či osob jednajících jménem a na účet subdodavatele v souvislosti s poskytováním Služeb,

b) proškolení zaměstnanců Poskytovatele a subdodavatele 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 subdodavatele na příslušném pracovišti“. Poskytovatel je však povinen zajistit účast příslušných zaměstnanců, popř. zaměstnanců subdodavatelů při školení a v případě, že uvedení zaměstnanci budou cizinci, zajistí Poskytovatel též, aby školení bylo pro uvedené zaměstnance zcela srozumitelné.

X.
Závěrečná ustanovení

10.1 Každá Smluvní strana je povinna nést veškeré náklady a výdaje, které jí vznikly v souvislosti s uzavřením dle Smlouvy sama.

10.2 Smluvní strany si ujednávají, že smlouva bude podepisována v elektronické podobě.

10.3 Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a účinnosti dnem jejího uveřejnění v registru smluv. Smluvní strany si současně ujednávají, že podle Smlouvy budou postupovat již od 1. 7. 2026. Závazek mlčenlivosti a ochrany důvěrných informací zůstává v platnosti i po ukončení Smlouvy.

10.4 Smlouva, jakož i práva a povinnosti vzniklé na základě Smlouvy nebo v souvislosti s ní, se řídí právním řádem České republiky, zejména Občanským zákoníkem v platném znění.

10.5 Smluvní strany prohlašují, že pokud se kterékoliv ustanovení Smlouvy nebo s ní související ujednání či jakákoli její část ukáží 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.

10.6 Veškeré spory mezi Smluvními stranami vzniklé ze 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.

10.7 Smlouvu lze doplňovat nebo měnit pouze písemnými, číslovanými dodatky, podepsanými všemi Smluvními stranami.

10.8 Smluvní strany prohlašují, že Smlouvu uzavřely ze své pravé, svobodné a vážně míněné vůle, nikoliv v tísni nebo za jinak nápadně nevýhodných podmínek. Dále Smluvní strany prohlašují, že si Smlouvu před jejím uzavřením pročetly, jejímu obsahu zcela porozuměly a bezvýhradně s ním souhlasí a na důkaz toho k ní připojují své podpisy.

10.9 Osobní údaje uvedené ve 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 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.

10.10 Poskytovatel se zavazuje při plnění Smlouvy dodržovat veškeré požadavky na kybernetickou bezpečnost vyplývající ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti, v platném znění, a jeho prováděcích předpisů.

10.11 Podpisem Smlouvy Objednatel stvrzuje, že se seznámil s dokumentem Poskytovatele „Požadavky kybernetické bezpečnosti na významné dodavatele“, který tvoří **Přílohu č. 4** Smlouvy. O případné aktualizaci bude informován Poskytovatelem e-mailem na kontaktní adresu: [redacted]

10.12 Smluvní strany berou na vědomí, že Poskytovatel je právnickou osobou, v níž má většinovou majetkovou účast územní samosprávný celek, a proto se na Smlouvu 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**“).

10.13 Smluvní strany se dohodly a souhlasí s tím, že Smlouvu uveřejní v Registru smluv pouze Poskytovatel, a to ve verzi pro uveřejnění, tj. po znečitelnění údajů (metadat), které tvoří obchodní tajemství, a to nejpozději do 30 dnů po podpisu Smlouvy.

Přílohy:

č. 1 – Katalog služeb (rozsah plnění)
č. 2 – Tým / role a pověřené osoby
č. 3 – Hodnocení rizik
č. 4 – Požadavky kybernetické bezpečnosti na významné dodavatele

V Plzni dne ……

Za Poskytovatele:

[redacted]

Plzeňská teplárenská, a.s.
na základě plné moci ze dne 21. 5. 2025

V Plzni dne ……

Za Objednatele:

Ing. Jiří Král
jednatel
Plzeňská teplárenská Energetické služby, s.r.o.

[redacted]

Plzeňská teplárenská, a.s.
na základě pověření ze dne 21. 5. 2025

Jakub Vojta, BBS
jednatel
Plzeňská teplárenská Energetické služby, s.r.o.

Příloha č. 1 – Katalog služeb (rozsah plnění)

- Výkon role manažera kybernetické bezpečnosti / koordinace kybernetické bezpečnosti pro Objednatele (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;
- 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 (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;
- vedení a aktualizace obsahu registru rizik kybernetické bezpečnosti v nástroji určeném Poskytovatelem, přičemž Poskytovatel zajistí pořízení a provoz tohoto nástroje a zpřístupnění potřebných účtů/přístupů Objednateli;
- 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 (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

- Poskytovatel zajistí pořízení, licencování a provoz nástroje pro evidenci registru rizik (včetně správy přístupů a dostupnosti nástroje). Objednatel nenese 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 (dodatek Smlouvy) dle pravidel sjednaných ve Smlouvě.

Příloha č. 2 – Tým / role a pověřené osoby

Tým

Jméno a příjmení	Role	E-mail	Telefon
[redacted]			

Role

Manažer kybernetické bezpečnosti – 1x

- Řízení a koordinace plnění smlouvy a priorit napříč subjekty,
- governance/reporting vedení, eskalace rizik a incidentů,
- schvalování metodik, výjimek.

Architekt kybernetické bezpečnosti – 1x

- Bezpečnostní architektura, security-by-design, posuzování změn a projektů,
- definice bezpečnostních požadavků, baseline, kompenzační opatření,
- podpora při auditech/posudcích (architektonická část).

Specialista kybernetické bezpečnosti – 1x

- Zpracování analýz rizik a správa obsahu registru rizik,
- koordinace evidence plnění opatření (akční body), podklady pro reporting,
- operativní podpora incident procesů (evidence, post-incident review podklady)

Příloha č. 3 - Hodnocení rizik

Dotazník aplikovaných opatření na straně SUBDODAVATELE
Název SUBDODAVATELE: EP Cybershield, s.r.o. (IČO: 28977921)

1	Otázka Soulad s legislativou	Odpověď	Poznámky
a.	Je SUBDODAVATEL orgánem nebo osobou povinnou dle zákona č. 181/2014 o kybernetické bezpečnosti anebo č. 264/2025 o kybernetické bezpečnosti?	NE	
b.	Má SUBDODAVATEL platnou certifikaci ČSN ISO/IEC 27001 na své informační a komunikační systémy?	NE	
c.	Aplikuje SUBDODAVATEL standard ČSN ISO/IEC 27001 na své informační a komunikační systémy (i bez platné certifikace)?	ANO	
d.	Byl SUBDODAVATEL určen významným dodavatelem dle vyhlášky č. 82/2018 Sb o kybernetické bezpečnosti nebo vyhlášky č. 409/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností i od jiných organizací, než je OBJEDNATEL?	NE	
2	**Systém řízení informační a kybernetické bezpečnosti**		
a.	Má SUBDODAVATEL stanovena pravidla pro ochranu dat, informací a technických aktiv?	ANO	
b.	Má SUBDODAVATEL vypracovanou dokumentaci s pravidly pro řízení bezpečnosti informací a kybernetické bezpečnosti?	ANO	
3	**Řízení aktiv**		
a.	Vede SUBDODAVATEL aktualizovanou evidenci všechn svých technických prostředků/aktiv (HW i SW)?	ANO	
b.	Má SUBDODAVATEL stanovena pravidla pro používání technických prostředků/aktiv?	ANO	
4	**Řízení rizik**		
a.	Řídí SUBDODAVATEL vlastní rizika na základě relevantních hrozeb a zranitelností?	ANO	
b.	Zpracovává SUBDODAVATEL pravidelně Zprávu o řízení rizik s obsahem dle 4.3.b) Přílohy č.3 SMLOUVY?	ANO	
c.	Kdy SUBDODAVATEL provedl naposledny aktualizaci analýzy rizik a vydal Zprávu o řízení rizik?	ANO	
5	**Organizační bezpečnost, bezpečnostní role a bezpečnost lidských zdrojů**		
a.	Má SUBDODAVATEL stanoveny pravomoci a odpovědnosti v rámci své organizace, vedoucí k zajištění kybernetické bezpečnosti?	ANO	
b.	Má SUBDODAVATEL určeny odpovědné osoby za oblast kybernetické bezpečnosti?	ANO	
c.	Provádí SUBDODAVATEL vzdělávání svých pracovníků pro zlepšení jejich bezpečnostního povědomí a zvýšení odbornosti?	ANO	
6	**Řízení dodavatelů**		
a.	Vede SUBDODAVATEL evidenci svých poddodavatelů, jejichž dodávky mají vliv na zajištění kybernetické bezpečnosti ZHOTOVITELE nebo jeho dodávek?	ANO	
b.	Vyžaduje SUBDODAVATEL po svých poddodavatelích požadavky na zajištění kybernetické bezpečnosti?	ANO	
7	**Řízení provozu a komunikací**		
a.	Provádí SUBDODAVATEL pravidelné zálohy, vč. kontroly použitelnosti a testu obnovení provedených záloh?	ANO	
b.	Řídí SUBDODAVATEL technické zranitelnosti svých provozovaných systémů?	ANO	
8	**Řízení změn**		
a.	Řídí SUBDODAVATEL významné změny, za které se považují změny na straně aktiv SUBDODAVATELE, které mají nebo mohou mít vliv na kybernetickou bezpečnost?	ANO	
9	**Řízení přístupu**		
a.	Dokumentuje SUBDODAVATEL přidělování uživatelských oprávnění?	ANO	
b.	Přiděluje SUBDODAVATEL pouze nezbytná minimální oprávnění?	ANO	
c.	Provádí SUBDODAVATEL pravidelné přezkoumání a úpravy přístupových oprávnění?	ANO	
10	**Akvizice, vývoj, údržba**		
a.	Zajišťuje SUBDODAVATEL bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které používá nebo nasazuje?	ANO	
b.	Dodržuje SUBDODAVATEL nejlepší praktiky pro bezpečný vývoj SW?	ANO	
11	**Zvládání kybernetických bezpečnostních událostí a incidentů**		
a.	Má SUBDODAVATEL stanoveny a aplikovány postupy pro detekci, hlášení a řešení kybernetických bezpečnostních incidentů na komunikační a informační infrastruktuře SUBDODAVATELE?	ANO	
b.	Má SUBDODAVATEL zaveden proces včasného informování osob zastávající bezpečnostní role o vzniku kybernetických bezpečnostních událostí?	ANO	
c.	Vede SUBDODAVATEL evidenci kybernetických bezpečnostních incidentů?	ANO	
d.	Byl u SUBDODAVATEL za posledních 24 měsíců zaznamenán bezpečnostní incident, který měl dopad na důvěrnost/dostupnost/integritu technických aktiv nebo informací?	NE	
12	**Kontrola a audit**		
a.	Provádí SUBDODAVATEL pravidelný audit (interní či externí) plnění opatření pro zajištění kybernetické bezpečnosti? Pokud ano, kdy byl naposledny proveden?	ANO	
b.	Provádí SUBDODAVATEL pravidelný audit (interní či externí) plnění opatření pro zajištění kybernetické bezpečnosti u svých poddodavatelů? Pokud ano, kdy byl naposledny proveden?	ANO	
13	**Kontinuita činnosti**		
a.	Má SUBDODAVATEL stanovenu minimální úroveň poskytovaných služeb pro zajištění požadovaného předmětu plnění?	ANO	
b.	Má SUBDODAVATEL vypracované, aktualizované a testované havarijní plány pro obnovu informačního a komunikačního systému?	ANO	
14	**Fyzická bezpečnost**		
a.	Má SUBDODAVATEL stanoven fyzický bezpečnostní perimetr?	ANO	
b.	Má SUBDODAVATEL stanovena pravidla a prostředky pro zamezení neoprávněného přístupu do vymezeného bezpečnostního perimetru?	ANO	
15	**Bezpečnost komunikačních sítí**		
a.	Má SUBDODAVATEL segmentovánu komunikační síť?	ANO	
b.	Řídí SUBDODAVATEL komunikaci (vč. blokování nežádoucí komunikace) na své síti?	ANO	
c.	Má SUBDODAVATEL zabezpečeny bezdrátové technologie a případný vzdálený přístup do své sítě?	ANO	

16	**Správa a ověřování identit, řízení přístupových oprávnění**		
a.	Má SUBDODAVATEL nástroj nebo proces pro správu identit uživatelů?	ANO	
b.	Má SUBDODAVATEL stanoveny požadavky na sílu hesla pro uživatele a administrátory?	ANO	
c.	Má SUBDODAVATEL stanovena pravidla pro postup při opakovaném neúspěšném přihlášení a dalších podezřelých aktivitách?	ANO	
17	**Ochrana před škodlivým kódemí**		
a.	Má SUBDODAVATEL spuštěnou a aktualizovanou antivirovou ochrany na všech prvcích informačního systému?	ANO	
b.	Mý SUBDODAVATEL zajištěnu ochranu proti škodlivému kódu na zařizeních, kde není možné antivirový	ANO	
18	**Detekce, sběr a vyhodnocení událostí v informačním systému**		
a.	Zaznamenává a uchovává SUBDODAVATEL důležité bezpečnostní a provozní údaje svých technických aktiv?	ANO	
b.	Zaznamenává a uchovává SUBDODAVATEL činnosti uživatelů důležité z hlediska bezpečnosti a ochrany	ANO	
c.	Má SUBDODAVATEL implementován proces nebo nástroj (SIEM apod.) pro detekci kybernetických bezpečnostních událostí/incidentů?	ANO	
19	**Aplikační bezpečnost**		
a.	Pokud je činností SUBDODAVATELE návrh a vývoj SW/aplikací, jsou při něm zohledňovány i požadavky kybernetické bezpečnosti?	N/A	

Příloha č. 4 – Požadavky kybernetické bezpečnosti pro významné dodavatele

Obsah:

Obsah: 1
1 Základní pojmy a zkratky 2
2 Úvodní ustanovení 2
3 Pravidla pro POSKYTOVATELE 3
3.1 Fyzická bezpečnost – pohyb v areálu OBJEDNATELE 3
3.2 Řízení do přístupu do sítě 3
3.3 Politika hesel 3
3.4 Požadavky na zařízení připojovaná do sítě OBJEDNATELE 4
3.5 Instalace SW 4
3.6 Výměnná paměťová média 4
3.7 Zakázané činnosti 4
3.8 Hlášení kybernetických bezpečnostních incidentů 5
3.9 Monitoring činností 5
3.10 Klasifikace a pravidla nakládání s informacemi 5
Příloha č. 1 PIKYB 6
Příloha č. 2 PIKYB 8
Příloha č. 3 PIKYB 10

1 ZÁKLADNÍ POJMY A ZKRATKY

SMLOUVA	Smlouva o dílo/Kupní smlouva/Rámcová smlouva o poskytování služeb jejíž přílohou je tento dokument.
SYSTÉM	Služby/dodávky specifikované v Předmětu DÍLA SMLOUVY a jejích přílohách.
OBJEDNATEL	Plzeňská teplárenská Energetické služby, s.r.o.
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 POSKYTOVATELE	Hmotné i nehmotné věci ve vlastnictví nebo nájmu POSKYTOVATELE, které jsou nezbytné k plnění předmětu smlouvy.
Prostředí POSKYTOVATELE	Fyzický perimetr určený ohraničením fyzického prostoru v nájmu nebo majetku POSKYTOVATELE anebo logický perimetr definovaný hraničními prvky informačního/komunikačního systému ve správě nebo majetku POSKYTOVATELE.
VoKB	Vyhláška č. 409/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
ZoKB	Zákon č. 264/2025 Sb., o kybernetické bezpečnosti
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

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

3 PRAVIDLA PRO POSKYTOVATELE

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

- s prostředky POSKYTOVATELE;
- s prostředky OBJEDNATELE;
- mimo prostředí OBJEDNATELE.

Při veškeré činnosti musí pracovník POSKYTOVATELE 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 POSKYTOVATELE oprávnění vstupovat pouze do prostor, které jsou nezbytné pro vykonávání jeho činnosti.

POSKYTOVATEL 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 POSKYTOVATELE nemusí být POSKYTOVATEL vpuštěn do areálu OBJEDNATELE.

3.2 Řízení do přístupu do sítě

Přidělení oprávnění přístupu do prostředí OBJEDNATELE pracovníkovi POSKYTOVATELE se řídí principem nezbytného minima a není nárokové.

Pracovník POSKYTOVATELE 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 POSKYTOVATELE evidována. Za sdílené autentizační prostředky odpovídá žádající osoba o výjimku na straně POSKYTOVATELE.

Přístupová oprávnění budou využívána výhradně k účelům splnění předmětu SMLOUVY.
Pokud má pracovník POSKYTOVATELE 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 POSKYTOVATELE 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 POSKYTOVATELE, 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 PTES), 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 POSKYTOVATELE 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 POSKYTOVATEL vykonává pro OBJEDNATELE. POSKYTOVATEL odpovídá za bezpečnost výměnných paměťových médií a jejich pravidelnou kontrolu po celou dobu projektu. O využívání výměnných médií souvisejících s předmětem DÍLA musí POSKYTOVATEL 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 POSKYTOVATELE je zakázáno:

- bez předchozí domluvy s odpovědným pracovníkem PTES 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 obejití 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

POSKYTOVATEL 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.

Přičemž K**ybernetickou 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).

A **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 POSKYTOVATELE k aktivům a infrastruktuře OBJEDNATELE jsou nepřetržitě zaznamenávány, monitorovány a vyhodnocovány.

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

3.10 Klasifikace a pravidla nakládání s informacemi

Pracovník musí dodržovat pravidla nakládání s informacemi dle jejich klasifikace (viz příloha č. 2 PIKYB – 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 POSKYTOVATELE řídit příslušným způsobem mazání a likvidace dat a informací dle jejich klasifikace (viz Příloha č. 3 PIKYB – Způsob mazání a likvidace dat a informací).

Příloha č. 1 PIKYB – Žádost o zřízení přístupu do sítě PTES

Žádost o zřízení přístupu do sítě Plzeňská teplárenská Energetické služby, s.r.o.

Základní informace o objednavateli			
Název společnosti:			
Jméno a příjmení žadatele[1]:			
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:	

Odpovědná osoba (garant) za PTES	
Jméno a příjmení:	
Funkce:	
Osobní číslo:	
Telefon:	

Požadavky na přístup	
Druh (popsat) požadovaného přístupu[2]:	
Aplikace/Server/PC[3]:	
Zařízení, která budou použita pro přístup (MAC adresa)[4]:	
Poznámky k upřesnění požadavku[5]:	

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 Energetické služby, s.r.o.).

Připojovat se do sítě PTES 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 PTES je zakázáno. Pokud je potřeba přenést data do zařízení společnosti PTES je povoleno jen po kontrole administrátorem a vždy jen na zařízeních (USB flash disk, externí disk atd.) v majetku PTES.

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

Společnost PTES 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 PTES 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 PTES (Garant)**

Příloha č. 2 PIKYB – 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**
Označení	Není vyžadováno. Dokumenty lze označit textem „**Veřejné**“ V případě sdílení nebo výměny dle TPL možno označit TLP:WHITE	Dokumenty označit textem „**Interní**“. V případě sdílení nebo výměny dle TPL možno označit TLP:GREEN nebo TLP:AMBER	Dokumenty označit textem „**Citlivé**“ nebo „**Důvěrné**“. V případě sdílení nebo výměny dle TPL možno označit TLP:AMBER	Dokumenty označit textem „**Vysoce citlivé**“ nebo „**Tajné**“. V případě sdílení nebo výměny dle TPL možno označit TLP:RED nebo TLP:AMBER
Přístup	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.
Uložení	Není vyžadována žádná ochrana.	Definované úložiště	Definované úložiště, může být šifrováno	Definované úložiště, které je šifrované.
Kopie	Není vyžadována žádná ochrana.	Není vyžadována žádná ochrana.	Informovat Garanta.	Písemné svolení Garanta.
Změny	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.
Pošta	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.
e-mail	Není vyžadována žádná ochrana.	Není vyžadována žádná ochrana. Pro interní nebo smluvní příjemce.	Kryptografické zabezpeční. Jen pro určené příjemce.	Kryptografické zabezpečení. Jen pro úzký a definovaný okruh příjemců.
LAN / WAN	Není vyžadována žádná ochrana.	Není vyžadována žádná ochrana.	Doporučené kryptografické zabezpeční přenosu dat komunikační sítí mimo uzavřené řídící systémy.	Kryptografické zabezpeční přenosu dat komunikační sítí.
Internet	Řízení přístupu, omezení přístupových práv pro zápis.	Řízení přístupu, omezení přístupových práv pro zápis.	Kryptografické zabezpeční.	Kryptografické zabezpečení.
Manipulace	Se svolením Garanta.	Se svolením Garanta.	Se svolením Garanta dle odsouhlaseného postupu.	Se svolením Garanta dle písemně odsouhlaseného postupu.

POŽADAVKY NA OCHRANU AKTIVA				
	ÚROVEŇ / HODNOCENÍ AKTIVA			
	1 - NÍZKÁ	2 - STŘEDNÍ	3 - VYSOKÁ	4 - KRITICKÁ
Zálohy / Dostupnost	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.

Příloha č. 3 PIKYB – 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.

ZPŮSOBY 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**
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.
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.

ZPŮSOBY 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**
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.