SPRÁVA ŽELEZNIC

Váš dopis zn.
Ze dne
Naše zn. 4294/2025-SŽ-SŽT-OPS
Listů/příloh 3/4

Vyřizuje Peter Koumal
Mobil +420 720 970 204
E-mail Koumal@spravazeleznic.cz

Datum 18.11. 2025

Pozvánka k předběžné tržní konzultaci ve věci přípravy zadávacích podmínek pro veřejné zakázky s názvy „Mobilní kontejnerové datové centrum" a "Realizace systému zabezpečeného úložiště v prostředí Správy železnic", případně pro jinou veřejnou zakázku shodnou s předmětem těchto dvou zakázek (dále jen „***Pozvánka***").

Vážená paní, vážený pane,

Správa železnic, státní organizace (dále jen „***Zadavatel***") Vás touto cestou informuje, že připravuje zadávací řízení na veřejné zakázky s názvy „Mobilní kontejnerové datové centrum" a "Realizace systému zabezpečeného úložiště v prostředí Správy železnic". Zadavatel současně zvažuje variantu sloučení předmětu plnění do jediné veřejné zakázky s navrhovaným názvem „Mobilní datové centrum a realizace systému zabezpečeného úložiště v prostředí Správy železnic". Zadavatel si vyhrazuje právo zvolit výslednou variantu realizace (jedna sloučená veřejná zakázka / dvě samostatné veřejné zakázky / popřípadě jiný počet), a to s ohledem na technickou návaznost veřejných zakázek, ekonomickou výhodnost a zachování soutěžního prostředí.

Vyhlášení veřejné zakázky/veřejných zakázek bude předcházet předběžná tržní konzultace (dále jen „***PTK***"), jejímž cílem bude získat relevantní informace pro správné nastavení předmětu plnění, zadávacích podmínek, volby druhu zadávacího řízení či způsobu hodnocení předložených nabídek. Zadavatel usiluje o získání kvalitního plnění, které bude splňovat jeho potřeby, a to za odpovídající cenu.

Konání jedné PTK tematicky pokrývající předmět obou plánovaných veřejných zakázek zvolil Zadavatel zejména s ohledem na technickou příbuznost poptávaného plnění a obdobný okruh potenciálních dodavatelů. Pro účely následného zadávacího řízení však Zadavatel aktuálně zvažuje různé varianty způsobu realizace.

Cílem veřejných zakázek/veřejné zakázky je uzavření smlouvy, jejímž předmětem bude pořízení mobilního modulárního datového centra, které bude definováno jako trvale bezobslužné pracoviště bez stálé fyzické obsluhy, realizované v kontejnerovém provedení a vybudování centralizovaného zabezpečeného datového úložiště v prostředí Správy železnic. Toto zahrnuje výběr technologie a implementaci řešení zabezpečeného úložiště včetně dodání potřebné infrastruktury (např. zálohovacích serverů a diskové kapacity pro vybrané informační systémy).

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČO: 709 94 234 DIČ: CZ 709 94 234
www.szdc.cz

Správa železniční telematiky
V Celnici 1028/10
110 00 Praha 1

Cílem PTK je transparentním způsobem získat přehled o současné situaci na trhu, možnostech dodavatelů a ujasnění otázek nezbytných pro realizaci veřejné zakázky.

PTK podle evropské zadávací směrnice (2014/24/EU) je možností zadavatele předtím, než vyhlásí veřejnou zakázku, komunikovat s dodavateli a zjišťovat (případně dalšími relevantními osobami) jejich možnosti a návrhy řešení. V rámci zvoleného modelu bude představen záměr zadavatele, včetně některých navrhovaných detailů jak předmětu veřejné zakázky, tak zadávacího řízení. Dodavatelé se pak budou moci k navrhovaným parametrům zakázky vyjádřit. Dojde tak ke zvýšení transparentnosti zadávacího řízení a získání relevantních a objektivních informací o možnostech trhu, tak aby mohl zadavatel optimálně nastavit zadávací podmínky veřejné zakázky, resp. celkové řešení zadávacího řízení. Vedení PTK je rovněž zcela v souladu s ust. § 33 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „***Zákon***").

Zadavatel v rámci PTK žádá o zodpovězení dotazů uvedených v Příloze č. 4 této Pozvánky.

Forma PTK: písemná (s možností pokračování písemnou nebo ústní formou, podle potřeb Zadavatele)

Způsob konání PTK:

V prvním kole PTK zašlou dodavatelé či odborné subjekty, jež projeví zájem o účast na této PTK, odpovědi na otázky uvedené v příloze č. 4 této Pozvánky na e-mailovou adresu uvedenou níže.

Zadavatel si v případě potřeby vyhrazuje možnost uskutečnit druhé kolo PTK, přičemž v rámci tohoto druhého kola může dojít za účelem konzultace zamýšleného řešení i k osobnímu setkání s jednotlivými dodavateli či odbornými subjekty. Zadavatel si vyhrazuje právo pozvat do druhého kola libovolný počet účastníků z kola předchozího, přičemž vždy bude postupovat tak, aby nedošlo ke zvýhodnění žádného z účastníků, zejména neposkytne účastníkům druhého kola žádné dodatečné informace.

Předpokládaný počátek plnění předmětu veřejných zakázek je 2. kvartál roku 2026, přičemž může být na základě PTK upraven.

V případě Vašeho zájmu o účast na této PTK zašlete, prosím, odpovědi na otázky uvedené v příloze č. 4 této Pozvánky na e-mailovou adresu:
cnitptk@spravazeleznic.cz

Dodavatel či odborný subjekt by ve své odpovědi měl uvést minimálně:

- název dodavatele a sídlo dodavatele;
- IČO dodavatele;
- jméno a funkce kontaktních osob, včetně kontaktních údajů (minimálně e-mail);
- odpovědi na přiložené otázky.

Svoji odpověď prosím doručte nejpozději do 5. 12. 2025.

Předběžná tržní konzultace nesmí vést k porušení základních zásad Zákona. Průběh i výsledek předběžné tržní konzultace bude zaznamenán ve zprávě vytvořené zadavatelem. Informace z předběžných tržních konzultací užité v zadávacích podmínkách zadané veřejné zakázky budou v souladu s § 36 odst. 4 Zákona v zadávací dokumentaci výslovně označeny, a to včetně osob, které se na výsledku podílely.

SŽ tuto Pozvánku uveřejnila na svém profilu zadavatele prostřednictvím elektronického nástroje E-ZAK, současně byly osloveny subjekty Zadavateli známé, jakožto potenciální dodavatelé. (https://zakazky.spravazeleznic.cz/).

Děkuji za spolupráci.

S pozdravem

Ing. Dalibor Fajkus
18.11.2025 15:21
Podepsáno
elektronicky

Ing. Dalibor Fajkus
ředitel Správy železniční telematiky

Přílohy:
Příloha č. 1 – Obecná specifikace předmětu plnění
Příloha č. 2 – Technická specifikace předmětu plnění – Mobilní kontejnerové datové centrum
Příloha č. 3 – Technická specifikace předmětu plnění – Realizace systému zabezpečeného úložiště v prostředí Správy železnic
Příloha č. 4 – Otázky k zodpovězení PTK

Příloha č. 1 Pozvánky – Obecná specifikace předmětu plnění

Předběžná tržní konzultace ve věci realizace Mobilního kontejnerového datového centra a Realizace systému zabezpečeného úložiště v prostředí Správy železnic

Správa železnic, státní organizace (dále jen „***SŽ***"), plánuje realizaci Mobilního datového centra a Realizaci systému zabezpečeného úložiště v prostředí Správy železnic. Cílem této předběžné tržní konzultace je získání relevantních informací o možných nebo vhodných řešeních mobilního datového centra a zabezpečeného úložiště, aby případné budoucí veřejné zakázky mohly být zadány dostatečně přesným, technologicky neutrálním a nediskriminačním způsobem, a současně postupem, který bude vyhovovat požadavkům a prostředí SŽ.

Záměr SŽ v oblasti Mobilního kontejnerového datového centra

Správa železnic plánuje pořízení mobilního kontejnerového datového centra typu „all-in-one", které umožní rychlou instalaci, opakovaný transport a provoz bez stálé obsluhy. Řešení zajistí vysokou dostupnost, bezpečnost a energetickou efektivitu pro ICT infrastrukturu.

Záměr SŽ v oblasti Realizace systému zabezpečeného úložiště v prostředí Správy železnic

Realizace centralizovaného zabezpečeného úložiště zapadá do strategického rámce zvyšování kybernetické bezpečnosti SŽ. Nové úložiště má zajistit konsolidaci a ochranu dat napříč vybranými informačními systémy a technologiemi organizace. Úložiště bude sloužit pro bezpečnou správu, ukládání a archivaci dat pro vybrané aplikace SŽ a vybrané průmyslové a řídicí technologie. Záměr vybudování tohoto úložiště je v souladu s požadavky na zajištění kybernetické bezpečnosti (včetně požadavků zákona č. 181/2014 Sb. a vyhlášky č. 82/2018 Sb.) a s opatřeními definovanými ve Studii proveditelnosti IROP pro danou aktivitu.

Cíl veřejných zakázek

Cílem připravovaných veřejných zakázek – Mobilní kontejnerové datové centrum a Realizace systému zabezpečené úložiště v prostředí Správy železnic – je pořízení kompaktního „all-in-one" řešení, v němž budou veškeré technologie integrovány přímo uvnitř modulu. Součástí záměru je také vybudování a implementace centralizovaného zabezpečeného datového úložiště, včetně dodávky potřebné infrastruktury a souvisejících služeb.

Hlavní cíle VZ pro „Mobilní kontejnerové datové centrum" jsou:

- **Zajistit standardizované, flexibilní a poměrně rychle nasaditelné řešení** v podobě mobilního kontejnerového datového centra, které bude odpovídat technickým i provozním požadavkům na umístění ICT technologií.

Hlavní cíle VZ pro „Realizace systému zabezpečeného úložiště v prostředí Správy železnic" jsou:

- **Zajištění vysoké dostupnosti dat** pomocí geograficky oddělených clusterů a replikace mezi lokalitami (geo-clustering), což minimalizuje riziko ztráty dat při výpadku jedné lokality.
- **Centralizované řízení přístupů a autentizace** ke všem uloženým datům – přístupy k datům budou spravovány jednotně a bezpečně, aby se zvýšila úroveň kontroly nad daty.

Správa železniční dopravní cesty, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.szdc.cz

Správa železniční telematiky
V Celnici 1028/10
110 00 Praha 1

- **Zabezpečené ukládání dat včetně šifrování a správy klíčů** – všechna data budou ukládána zabezpečeně, s využitím šifrování a **Hardware Security Module (HSM)** pro správu šifrovacích klíčů.
- **Zvýšení odolnosti vůči výpadkům a incidentům** – infrastruktura úložiště bude navržena s ohledem na odolnost (disaster recovery), včetně záložních napájecích systémů a monitoringu prostředí, aby byla zajištěna kontinuita provozu i při nenadálých událostech.

Požadavky na řešení

Předběžné požadavky na řešení se nachází v dokumentaci, která je přílohou Pozvánky k PTK viz příloha č. 2 – *Technická specifikace předmětu plnění – Mobilní kontejnerové datové centrum* a příloha č. 3 – *Technická specifikace předmětu plnění – Realizace systému zabezpečeného úložiště v prostředí Správy železnic*.

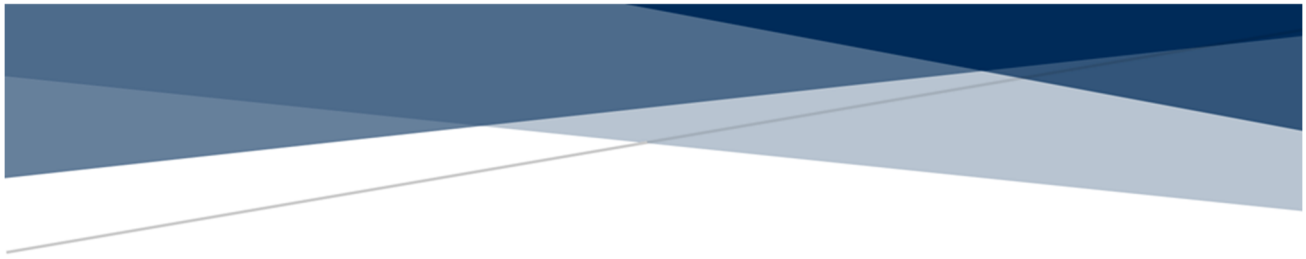
Předpokládaný postup

S ohledem na komplexnost řešení zabezpečeného úložiště SŽ předpokládá následující hlavní kroky realizace veřejných zakázek/veřejné zakázky:

- **Výběr technologie a detailního řešení:** Na základě výsledků PTK a interních podkladů proběhne výběr konkrétní technologie a architektury zabezpečeného úložiště. To zahrnuje volbu dodavatele hardware (disková pole, servery, kontejnerové datové centrum) a software (řídicí software úložiště, případně potřebné licence pro integraci, šifrování apod.), který nejlépe vyhoví definovaným požadavkům a zapadne do ICT prostředí SŽ. Důraz bude kladen na technologickou neutralitu při zachování potřebné úrovně zabezpečení a výkonu.
- **Dodávka a implementace řešení úložiště:** Vybraný dodavatel zajistí dodání veškerého potřebného vybavení a jeho instalaci. V této fázi dojde k fyzickému zřízení a zprovoznění mobilního datového kontejneru, instalaci diskových úložišť, serverů a síťových prvků, a nasazení softwarových komponent (řídicí software úložiště, integrace HSM, nastavení šifrování, propojení s IdM atd.). Součástí bude konfigurace úložiště podle požadovaných parametrů (nastavení storage tiering, zásad retence dat, zálohovacích politik apod.), otestování vysoké dostupnosti (výpadky a obnova) a bezpečnostních mechanismů.
- **Postupné připojení a migrace systémů:** Po zprovoznění infrastruktury budou na nové úložiště napojeny definované systémy a agendy. Předpokládá se migrace či centralizace dat ze **stávajících systémů** do nového úložiště. Tento krok bude vyžadovat úzkou spolupráci s garanty jednotlivých aplikací a systémů – cílem je minimalizovat dopad na provoz a ověřit, že všechny aplikace mohou s novým úložištěm komunikovat bez problémů (kompatibilita protokolů, dostatečná propustnost sítě, latence atd.). V rámci této fáze dojde i k implementaci potřebných integračních vazeb, jako je napojení úložiště na IdM/PAM pro řízení přístupů, integrace s monitorovacími nástroji a SIEM pro dohled nad bezpečnostními událostmi a dalšími podpůrnými systémy.
- **Zajištění podpory a provozu:** Po úspěšné implementaci bude nastaven model provozu a podpory úložiště. To zahrnuje zaškolení administrátorů SŽ (popř. převzetí do režimu služby, pokud by byl dodavatel zajišťovatelem provozu), definici provozní dokumentace, nastavení procesů pro běžnou údržbu i řešení incidentů. Dodavatel by měl poskytnout záruky a podporu po dohodnutou dobu, včetně pravidelných aktualizací systémového software, bezpečnostních záplat a případného rozšiřování kapacit dle potřeb SŽ. Součástí plnění budou také veškeré **dokumentační výstupy** (uživatelské příručky, administrátorská dokumentace, popisy konfigurace, bezpečnostní politika úložiště apod.), nutné certifikace zařízení a případně návrhy provozních smluv (SLA) pro zajištění spolehlivého chodu úložiště.

Předpokládá se, že výsledkem realizace této aktivity bude plně funkční **centrální zabezpečené úložiště dat** zahrnující veškerý potřebný hardware, software a služby, které naplní výše uvedené požadavky. Úložiště formou mobilního datového kontejneru výrazně zvýší úroveň zabezpečení dat Správy železnic a vytvoří základ pro další iniciativy v oblasti digitalizace a bezpečnosti informací. Dodavatelé v rámci PTK pomohou svými odpověďmi upřesnit parametry řešení tak, aby následná zadávací dokumentace veřejné zakázky byla optimálně nastavena.

SPRÁVA ŽELEZNIC



SPRÁVA ŽELEZNIC

Mobilní kontejnerové datové centrum

(Příloha č. 2 Pozvánky - Technická specifikace předmětu plnění)

SPRÁVA ŽELEZNIC

Obsah dokumentu

Specifikace mobilního kontejnerového datového centra

1.1 Shrnutí požadovaných vlastností

Mobilní modulární datové centrum bude definováno jako trvale bezobslužné pracoviště bez stálé fyzické obsluhy, realizované v kontejnerovém provedení. Vzhledem k prostorovým možnostem je požadováno řešení s **mobilní samonosnou konstrukcí**, která umožní snadné usazení, opakovaný transport a přemístění na jinou lokalitu. Modul musí být navržen tak, aby jeho konstrukce umožňovala flexibilní manipulaci bez nutnosti zásadních stavebních úprav. Všechny stěny modulu musí být **tepelně izolovány** tak, aby vyhovovaly extremním klimatickým podmínkám České republiky od **−19 °C do +39 °C** pro standardní HVAC návrhy dle ASHRAE institutu.

Datové centrum bude dodáno jako kompaktní „all-in-one" řešení, v němž budou veškeré technologie integrovány přímo uvnitř modulu. Na místě instalace mobilního kontejnerového datového centra proběhne tzv. FAT test (Factory Acceptance Test), který ověří funkčnost zařízení při **maximálním** jmenovitém výkonu IT infrastruktury. Test bude proveden po dobu **48 hodin** za použití simulované odporové zátěže a za účasti zástupce Zadavatele.

Instalace bude provedena na předem připravené betonové patky, bez nutnosti složitých stavebních nebo instalačních prací – pouze s připojením na připravené napájecí a komunikační kabeláže.

Součástí řešení musí být pokročilý systém dálkového monitoringu, který umožní reálný časový sběr, vyhodnocování a vizualizaci klíčových provozních dat z technologií a senzorů. Dodavatel musí zajistit integraci požadovaných dat v definovaném formátu do nadřazeného monitorovacího systému provozovaného Zadavatelem.

Základní požadované technické parametry:

1.1.1 Mobilní datacentrový modul – technické požadavky

- **Vizuální identita:** Barevné provedení modulu a umístění identifikačních prvků (např. logo provozovatele) musí být v souladu s vizuálním stylem provozovatele;
- **Rozměrové požadavky:** Modul musí být navržen tak, aby umožňoval bezpečné a funkční umístění všech požadovaných technologií, bez nutnosti pevně stanovených rozměrů;
- **Konstrukce:** Modul bude vybaven ocelovou samonosnou konstrukcí s tepelnou izolací a plechovým opláštěním, která zajistí mechanickou stabilitu při osazení, přepravě a manipulaci;
- **Vstupní komora:** Součástí modulu bude integrovaná vstupní komora (podpůrná místnost), která bude fyzicky oddělovat datový sál od venkovního prostředí, čímž se zajistí ochrana proti klimatickým vlivům;
- **Umístění technologií:** Technologické komponenty, jako je například systém chlazení, musí být umístěny tak, aby nebyly pohledově exponované. Preferovaným řešením je jejich instalace ve střešní části modulu;
- **Klasifikace infrastruktury:** Vnitřní Non-IT infrastruktura musí odpovídat klasifikaci dle Uptime Institute, přičemž řešení musí splňovat požadavky na úroveň **TIER III**;
- **Příkon ICT:** Plánovaný příkon ICT technologií činí **100 kW**;
- **Celkový příkon:** Celkový příkon mobilního datového centra, včetně Non-IT technologií (např. chlazení, dobíjení baterií), nesmí překročit **180 kW;**
- **Napájení:** Pro napájení modulu musí být v lokalitě k dispozici **samostatný třífázový přívod** s jištěním **315 A;**

- **Instalace elektro a datové infrastruktury:** Elektrická instalace a datová kabeláž musí být realizovány v souladu s platnými technickými a požárními normami, s důrazem na zajištění mechanické stability během přepravy a manipulace;
- **Osvětlení:** Osvětlení bude realizováno pomocí energeticky úsporných svítidel. V jednotlivých místnostech bude osvětlení ovládáno místními nástěnnými vypínači, umístěnými u vstupních dveří. Venkovní osvětlení bude řízeno automatizovaným systémem;
- **Energetická efektivita:** Průměrná roční hodnota PUE (Power Usage Effectiveness) nesmí překročit **1,3**
- **Datové rozvaděče (RACKy):**
  - Datové centrum bude vybaveno **minimálně 8 rozvaděči** typu RACK o rozměrech **42U × 800 mm × 1200 mm**;
  - Každý rozvaděč bude vybaven zamykacími jednodílnými dveřmi v přední části a dělenými dveřmi v zadní části;
  - Maximální garantovaný výkon na jeden RACK bude **10 kW**;
  - Nosnost (dynamické zatížení) rozvaděče bude minimálně **1300 kg**;
  - Pro zaslepení volných pozic budou dodány záslepky v provedení pro bez nástrojovou montáž pro **80** % U pozic**;**
- **Napájení RACKů:**
  - Každý RACK bude vybaven minimálně čtveřicí PDU (Power Distribution Unit);
  - Dvě třífázové PDU (32 A) ve spodní části racku:
    - Minimálně 8x C19 zásuvek a minimálně 8x C13 zásuvek
  - Dvě jednofázové PDU (16 A) v horní části racku:
    - Minimálně 4x C19 zásuvek a minimálně 12x C13 zásuvek
  - PDU musí být měřené a monitorované, s možností sledování odběru a stavu napájení, a musí obsahovat dostatečný počet zásuvek pro připojení všech ICT zařízení v plně osazeném racku;
- **Vnitřní strukturovaná kabeláž:**
  - RACKy budou vzájemně propojeny:
    - Optickou předkonektorovanou kabeláží – minimálně **12** portů, standard OM4, MM, duplex, LC/UPC
    - Metalickou kabeláží – minimálně **6** portů, kategorie CAT 6a, FTP/SFTP
  - Jeden RACK bude vyhrazen jako **LAN RACK** pro ukončení a správu síťové konektivity
- **Chlazení:**
  - Chladicí systém bude navržen pro spolehlivý provoz v kontejnerovém prostředí, s požadavkem na redundanci minimálně v konfiguraci **N+1.** Umístění venkovních chladicích jednotek bude řešeno s ohledem na prostorové a provozní nároky; preferováno je střešní umístění, integrované do konstrukce modulu tak, aby nebyly pohledově exponované;
  - Chladící systém musí mít minimálně dva oddělené chladící okruhy, umožňující provádět údržbu bez ovlivnění provozu;
  - Jednotky spolu musí komunikovat a předcházet cyklování.

- **UPS systém:**
  - Datové centrum bude vybaveno **dvěma oddělenými modulárními UPS systémy** v konfiguraci **N+1;**
  - Bateriová záloha musí zajistit minimálně **10 minut** provozu při zatížení **100 kW** pro každou UPS;
  - UPS musí být navrženy v **DPA** architektuře (Decentralized Parallel Architecture) – každý modul bude mít samostatné řízení, usměrňovač, střídač a statický přepínač (static switch);
  - UPS musí obsahovat appliance server pro bezpečné vypínání diskových polí.

- **Monitorovací systém prostředí:**
  - V datovém centru bude umístěn lokální dohledový server;
  - Systém musí zajišťovat kompletní monitoring všech Non-IT technologií umístěných v datovém centru;
  - Výstupy z monitorovacího systému musí být okamžitě dostupné přes zabezpečené webové rozhraní (HTTPS) po zprovoznění komunikační trasy a konfiguraci;
  - Monitorovací systém musí být integrovatelný do nadřazeného systému Zabbix, provozovaného Zadavatelem. A zároveň musí poskytnout možnost napojení na systém dálkové diagnostiky DDTS provozovaného Zadavatelem.

1.1.2 Silový přívod

Napájení mobilního datového centra bude zajištěno ze stávající distribuční rozvodny. Záložní napájení prostřednictvím **motorgenerátoru** není součástí tohoto řešení a bude řešeno samostatně mimo rámec této dodávky.

1.1.3 Bezpečnostní systémy mobilního datového centra

- **Poplachový zabezpečovací a tísňový systém (PZTS):**
  - Detekce pohybu bude zajištěna pomocí duálních detektorů (PIR + MW) umístěných ve studené a teplé uličce a v podpůrné místnosti;
  - Magnetické dveřní kontakty budou instalovány na vnitřních i vnějších dveřích;
  - Plášťová ochrana datové a podpůrné části bude realizována pomocí infrazávor nebo laserových detektorů, zajišťujících střežení obvodových stěn;
  - **Elektronická kontrola vstupů (EKV) – integrovaná do PZTS:**
    - Přístup bude zajištěn pomocí bezkontaktních čteček karet, v kombinaci s číselným PIN kódem;
    - Venkovní dveře budou osazeny pouze čtečkou karet s podsvícenou klávesnicí, minimálně ve bezpečnostní třídě RC3 dle ČSN EN 1627;
    - Vnitřní dveře do datového sálu budou vybaveny čtečkou karet s podsvícenou klávesnicí
    - Dveře budou osazeny elektromechanickým zámkem s bezpečnostním kováním typu koule–klika (klika směrem do chráněného prostoru) a bezpečnostní cylindrickou vložkou;
    - Přístupovým systémem (EKV) bude integrovaný do centrálního bezpečnostního systému ASSET Zadavatele. Správu a řízení přístupu bude zastřešovat Odbor bezpečnosti a krizového řízeni (O30) Správy železnic.

- **Dohledový kamerový systém (CCTV)**:
  - Kamery budou umístěny ve studené a teplé uličce, v podpůrné místnosti a nad venkovními dveřmi; podpora video analytiky na kameře.
  - Kamery budou umístěny i na plášti kontejneru a to tak, aby obsáhly celý prostor okolo kontejneru. Kamery budou rovně obsahovat video analytické funkce.
  - Online záběry všech kamer budou svedeny do video management systému O30.
  - Záznam bude uchováván na úložišti umístěném v datovém centru.
- **Stabilní hasicí zařízení (GHZ):**
  - Pro hašení bude použit autonomní hasicí systém, který v případě požáru zaplní prostor vhodným hasicím médiem (např. NOVEC 1230, FK-5-1-12, FM-200, Inergen);
  - Pro hašení baterií UPS bude použit vhodní detekční systém kouře a senzory plamene v prostoru UPS. A autonomní hasicí systém (např. Vermikulitový nebo F-500 systém) používající zónové hašení pouze v postižené části;
  - Detekce požáru bude zajištěna pomocí opticko-kouřových detektorů, doplněných o včasnou laserovou detekci.

1.2 Architektonické, vizuální a materiálové řešení

Navržená konstrukce modulu (kontejnerového datového centra) musí splňovat aktuální požadavky na ochranu životního prostředí a být v souladu s platnými technickými normami, bezpečnostními, hygienickými a požárními předpisy. Exteriér modulu bude vizuálně zpracován pomocí fasádního opláštění z ocelových profilů.

Datové centrum bude realizováno jako modulární kontejnerová technologie, která poskytuje výkonné, flexibilní a energeticky efektivní řešení s možností rychlého nasazení v řádu několika týdnů. Předpokládá se využití hotové konfigurace optimalizované z hlediska výkonu a hustoty, která umožní agilní rozšíření kapacity nebo upgrade koncové infrastruktury.

Modulární kontejnerové datové centrum musí být navrženo tak, aby bylo jako celek kompletně sestaveno a technologicky integrováno ve výrobním závodě. To zahrnuje instalaci všech non-IT technologií, jako jsou systémy napájení, záložní zdroje (UPS), rozváděče, chlazení, strukturovaná kabeláž, osvětlení, monitorovací a bezpečnostní systémy. Konstrukce modulu musí umožnit bezpečnou přepravu s již nainstalovanými zařízeními ve stojanech. Mechanická odolnost musí odpovídat požadavkům pro kamionovou dopravu dle doporučení ISTA (International Safe Transit Association).

Modul bude mít samonosnou konstrukci, která umožní snadné usazení, opakovaný transport a přemístění na jinou lokalitu bez nutnosti zásadních stavebních úprav.

Vizuální provedení modulu musí odpovídat jednotnému vizuálnímu stylu provozovatele (SŽ), jak je definováno v manuálu vizuální identity (Správa železnic – Logomanuál). Modul bude mít bílou barvu, logo provozovatele v barevném provedení o rozměrech 80 x 40 cm bude umístěno na obou delších stranách kontejneru (celkem 2 kusy). Logo musí být demontovatelné běžným nářadím.

Na stěně modulů, na levé straně venkovních dveří modulu ve výšce 150 cm na zemí bude umístněná památeční tabule, nerezová gravírovaná plaketa, o rozměru 30 x 20 cm. Text památeční tabule dodá Zadavatel 2 týdny před předáním modulárního datového centra Zadavateli.

1.3 Dispoziční a provozní řešení

Mobilní datové centrum je koncipováno jako trvale bezobslužné pracoviště, bez stálé fyzické obsluhy. Představuje řešení pro uživatele s požadavky na rychlou implementaci, mobilitu a nízké prostorové nároky. Veškerá infrastruktura datového centra je integrována do **jednoho modulárního kontejneru**, který zahrnuje jak ICT zařízení, tak podpůrné technologie nezbytné pro jeho provoz.

Modul je dispozičně rozdělen na dvě hlavní části:

- **Přechodová místnost**, která slouží jako vstupní místnost z venku pro zamezení přenosu nečistot do vnitřní místnosti s ITC technologiemi, příruční sklad a také pro umístění některých technologických zařízení (např. elektrické rozvaděče);
- **Prostor s ICT technologií**, kde jsou umístěny datové rozvaděče.

Toto uspořádání zajišťuje dodatečnou úroveň zabezpečení datového sálu a zároveň minimalizuje vnikání vlhkosti, prachu a dalších nečistot do prostoru s ICT.

Vstupní koridor slouží jako přechodová zóna mezi vnějším prostředím a ICT částí. Z koridoru je umožněn přístup do ICT prostoru.

Vstup do modulu je realizován přes dveře vybavené elektromechanickým zámkem s cylindrickou vložkou, ovládaným vnější bezkontaktní čtečkou s podsvícenou klávesnicí. Podpůrná místnost obsahuje podpůrné technologie a je vybavena kamerovým dohledem.

Přístup do ICT části je řízen pomocí elektronického přístupového systému, konkrétně čipovou kartou, v kombinaci s číselným PIN kódem. V této části se nachází jedna souvislá řada datových rozvaděčů, tvořící hlavní technologické jádro datového centra.

1.4 Bezbariérové užívání datového centra

S ohledem na provozní charakter, konstrukční řešení a vnitřní dispozici mobilního datového centra není umožněn přístup osobám s omezenou schopností pohybu a orientace. Modul není navržen pro bezbariérové užívání.

1.5 Umístnění mobilního modulu a základové konstrukce

Mobilní modul datového centra je možné instalovat jak na zpevněné, tak na nezpevněné části pozemku. V případě umístění na nezpevněný terén dodavatel provede základové a výkopové práce, které zajistí stabilitu a správné usazení modulu.

Modul musí být vybaven samonosnou konstrukcí, která umožňuje snadnou instalaci, opakovaný transport a přemístění bez nutnosti zásadních stavebních úprav. Instalace musí být provedena na vhodný podklad:

- **Na nezpevněném terénu**: pomocí silničních panelů nebo betónových patek, které zajistí rovnoměrné rozložení hmotnosti a stabilitu modulu.
- **Na zpevněném povrchu**: na existující asfaltové nebo betonové povrchy přímo bez nutnosti dalších stavebních úprav.

Základové pasy musí být umístěny pod rohovými patkami modulu a ve středové části konstrukce. Modul musí být usazen ve vodorovné poloze, přičemž maximální přípustný sklon nesmí překročit 1°.

Napájecí kabely, potrubí a další inženýrské sítě musí být vedeny mimo základové pasy, případně integrovány do konstrukce pasu tak, aby nedošlo k narušení jeho statické funkce.

1.6 Požadavky na finální povrchy v exteriéru

V případě instalace modulu datového centra na zpevněné plochy (např. asfaltové nebo betonové povrchy) musí být zajištěna rovinnost podkladu s tolerancí ±5 mm. Modul bude uložen přímo na tento povrch bez nutnosti dalších stavebních úprav.

Při umístění na nezpevněné části pozemku je nutné provést zpevnění a vyrovnání povrchu pomocí silničních panelů o tloušťce 150 mm. Panely budou použity ve dvou úrovních únosnosti:

- **20 t** v místech uložení modulu datového centra,
- **6 t** v plochách určených pro pochozí komunikaci.

Silniční panely musí být uloženy tak, aby navazovaly na okolní terén a nevytvářely výškové rozdíly. Rovinnost uložených panelů musí odpovídat požadavkům na zpevněné povrchy, tj. ±5 mm.

Zajištění stavební připravenosti dle tohoto bodu není předmětem této veřejné zakázky a bude realizováno samostatně Zadavatelem. V rámci dodávky je Dodavatel povinen zajistit vhodná opatření pro bezpečný přístup do modulu, v souladu s platnými normami – například protiskluzovou nástupní plochu nebo schodiště.

1.7 Oplocení prostoru datového centra

Oplocení prostoru, ve kterém bude umístěn modul datového centra, není součástí této veřejné zakázky. Případné řešení oplocení bude zajištěno samostatně Zadavatelem (SŽ).

Konstrukční a stavebně technické řešení mobilního datového centra

Mobilní datové centrum musí být navrženo tak, aby umožňovalo bezpečné a efektivní umístění veškeré potřebné technologie v rámci jednoho modulárního kontejneru. Modul musí disponovat samonosnou konstrukcí, která usnadňuje jeho instalaci, opakovaný transport a přemístění na jinou lokalitu bez nutnosti zásadních stavebních úprav.

Veškerá ICT infrastruktura a související podpůrné technologie nezbytné pro provoz datového centra budou integrovány do jednoho konstrukčního celku. Modul tvoří uzavřený skelet, který zajišťuje ochranu a provozuschopnost zařízení během provozu i přepravy.

1.8 Svislé konstrukce

Svislé konstrukce modulu datového centra budou tvořeny z ocelových svařovaných ohýbaných profilů a tvarovaných plechů. Vnitřní strana konstrukce bude provedena z ocelových plechů, které budou pevně uchyceny k nosnému ocelovému rámu modulu. Konstrukce musí zajistit dostatečnou tuhost, odolnost vůči mechanickému namáhání a splňovat požadavky na bezpečnost a životnost v souladu s platnými technickými normami.

1.9 Nosné konstrukce

Nosná konstrukce modulu datového centra je tvořena svařovaným rámem z ocelových ohýbaných profilů a tvarovaných plechů. Spodní a horní rámová část jsou vzájemně propojeny ocelovými profily, které zajišťují celkovou tuhost a stabilitu konstrukce.

Stěny modulu jsou tvořeny z profilovaných ocelových plechů, pevně uchycených k nosnému rámu. Tloušťka použitých ocelových prvků se liší v závislosti na konkrétní části konstrukce a požadované mechanické odolnosti:

- **Stěny a střecha**: standardní tloušťka oceli je 1,6 až 2 mm,
- **Rám podlahy a příčníky**: zesílená ocel o tloušťce 4 až 4,5 mm pro zajištění nosnosti při vysokém zatížení,
- **Rohové sloupky**: nejvyšší konstrukční pevnost, tloušťka oceli přesahuje 6 mm.

Konstrukce musí splňovat požadavky na statickou bezpečnost, odolnost vůči vibracím a nárazům při přepravě, a zároveň umožnit opakovanou instalaci bez ztráty funkčnosti.

1.10 Obvodový plášť

Obvodový plášť modulu datového centra musí být navržen tak, aby odolával povětrnostním vlivům typickým pro klimatické podmínky České republiky dle ASHRAE. Konstrukce pláště bude provedena z vysoce odolné oceli, která zajistí mechanickou pevnost a dlouhodobou životnost při provozu i přepravě.

Panely tvořící obvodový plášť budou žebrované, vodotěsné a odolné vůči povětrnostním vlivům. Konstrukce musí splňovat požadavky na ochranu proti vlhkosti, teplotním výkyvům a mechanickému poškození, a zároveň zajistit bezpečné provozní podmínky pro vnitřní technologii.

1.11 Vnitřní dělící konstrukce

Vnitřní dělící konstrukce modulu datového centra budou tvořeny sendvičovými panely s izolační vrstvou z polyuretanové pěny, překrytou lakovaným ocelovým plechem. Konstrukce stěn bude navržena tak, aby minimalizovala vznik tepelných mostů a tím omezila riziko kondenzace vlhkosti, zejména v zimních měsících.

Vnitřní dělící konstrukce musí splňovat požární odolnost dle normy ČSN EN 13501-2 nebo obdobné.

Stěny budou vyztuženy pomocí ocelových plechů a profilů, které umožní instalaci zařízení s vyšší hmotností, jež nelze kotvit přímo do základní konstrukce modulu. Celkové provedení musí zajistit mechanickou stabilitu, tepelnou izolaci a splňovat požadavky na bezpečný provoz ICT technologií.

1.12 Vodorovné konstrukce

Vodorovné konstrukce modulu datového centra budou tvořeny svařovanými ocelovými ohýbanými profily a tvarovanými plechy. Nosný rám spodní a horní části modulu bude vzájemně propojen ocelovými profily, které zajistí celkovou stabilitu a tuhost konstrukce.

Stěny modulu budou tvořeny z profilovaných ocelových plechů, pevně uchycených k nosnému rámu. Konstrukce musí být navržena tak, aby odolávala mechanickému zatížení při provozu i přepravě, a zároveň umožňovala bezpečné osazení technologických komponent.

1.13 Nosné konstrukce stropu

Nosná konstrukce stropu modulu datového centra bude tvořena svařovaným rámem z ocelových ohýbaných profilů a tvarovaných plechů. Spodní a horní rámová část modulu jsou propojeny ocelovými profily, které zajišťují celkovou stabilitu konstrukce.

Střešní panely budou standardně vyrobeny z kovových materiálů, přičemž je možné využít i alternativní materiály za předpokladu, že splňují požadavky na tepelnou regulaci nebo přispívají ke snížení celkové hmotnosti modulu.

Stropní konstrukce musí být navržena tak, aby:

- zajistila dostatečnou nosnost pro plánované technologické vybavení, zejména venkovní jednotky chladicího systému,
- umožnila rovnoměrné rozložení zatížení a provozní stabilitu,
- poskytovala odpovídající tepelnou izolaci,
- umožnila bezpečný pohyb obsluhy a instalaci zařízení na střeše modulu.

1.14 Podlahy

Podlahová konstrukce modulu datového centra bude tvořena vyztuženým ocelovým rámem, složeným z ohýbaných ocelových profilů. Povrch podlahy bude tvořen konstrukční deskou (např. CETRIS), která bude překryta antistatickým PVC povrchem, zajišťujícím bezpečný provoz ICT technologií.

Zateplení podlahy bude provedeno pomocí vrstvy polyuretanové pěny, která zajistí požadovanou tepelnou izolaci. Konstrukce podlahy musí být navržena tak, aby:

- poskytovala dostatečnou nosnost pro plánované technologické vybavení,
- umožňovala rovnoměrné rozložení zatížení a provozní stabilitu,
- splňovala požadavky na tepelnou izolaci a bezpečný pohyb obsluhy,
- umožňovala bezproblémovou instalaci zařízení.

1.15 Klempířské konstrukce

Klempířské konstrukce budou součástí vnitřního vybavení modulu datového centra a budou sloužit jako pomocné konstrukční prvky pro upevnění technologických zařízení. Tyto prvky musí být navrženy tak, aby umožňovaly bezpečnou a stabilní instalaci komponent s různou hmotností a rozměry, v souladu s požadavky na provozní spolehlivost a ergonomii.

1.16 Tepelné a zvukové izolace

Stěny modulu datového centra budou tvořeny sendvičovými panely s izolační vrstvou z polyuretanové pěny, překrytou lakovaným ocelovým plechem. Tepelná izolace bude navržena tak, aby účinně omezovala přenos tepla mezi vnějším a vnitřním prostředím modulu, čímž přispěje ke stabilizaci provozních podmínek ICT technologií.

Součástí konstrukce bude také akustická izolace, která sníží přenos hluku z okolí a omezí dozvuk uvnitř modulu. V případě potřeby bude použita kombinovaná tepelně-akustická izolace, která zajistí účinnou ochranu proti tepelným ztrátám i hlukové zátěži.

1.17 Výplně otvorů

Veškeré prostupy pro kabelové a potrubní vedení budou osazeny rozebíratelnými protiprachovými a protipožárními průchodkami. Každá průchodka bude dimenzována s minimální rezervou 30 % pro budoucí rozšíření technologické infrastruktury.

Prostupy pro napájecí a datové kabely budou vedeny buď spodní částí modulu, nebo boční stěnou, v závislosti na konkrétním technickém řešení a umístění modulu na lokalitě. Konstrukce prostupů musí být navržena tak, aby umožňovala bezpečnou instalaci, snadnou údržbu a splňovala požadavky na požární bezpečnost.

1.18 Venkovní protidešťové žaluzie

Veškeré prostupy vzduchotechniky (VZT) skrz obvodový plášť modulu datového centra budou osazeny venkovními protidešťovými žaluziemi. Žaluzie budou instalovány do rámů tvořených ocelovými profily a musí být navrženy tak, aby účinně zabránily vnikání dešťové vody do vnitřních prostor modulu, a zároveň neomezovaly funkčnost vzduchotechnického systému.

1.19 Vnitřní výplně otvorů – dveře

Hlavní vstupní dveře do modulu (včetně zárubní) datového centra budou mít minimální šířku 900 mm, výšku 2100mm a budou odpovídat bezpečnostní třídě RC3 dle normy ČSN EN 1627. Dveře budou tepelně izolované, vybavené elektromechanickým zámkem s funkcí anti-panik, bezpečnostním kováním typu koule–klika (klika umístěna v chráněném prostoru), bezpečnostní cylindrickou vložkou a přístupovým systémem s bezkontaktní čtečkou karet s podsvícenou klávesnicí. Nad vstupem bude instalována ochranná stříška proti dešti a sněhu.

Vstupní místnost (podpůrná místnost) bude od datového sálu oddělena pevnou dělící příčkou, která zajistí fyzickou bezpečnost, zabrání vniknutí nečistot a omezí nekontrolovanou výměnu vzduchu mezi prostory.

Vnitřní dveře mezi vstupní místností a datovým sálem budou rovněž mít minimální šířku 900 mm, výšku 2100mm, vybaveny elektromechanickým zámkem s funkcí anti-panik, čtečkou karet s podsvícenou klávesnicí.

Pro zajištění efektivního řízení proudění vzduchu budou prostory teplé a studené uličky stavebně odděleny. Vstup do prostoru teplé uličky bude zajištěn posuvnými dveřmi s mechanickou aretací, pro kontrolovanou separaci proudění vzduchu a optimalizaci chlazení.

1.20 Konstrukce zámečnické

Zámečnické konstrukce budou instalovány uvnitř modulu datového centra jako pomocné konstrukční prvky pro upevnění technologického vybavení. Tyto prvky musí být navrženy tak, aby umožňovaly bezpečnou a stabilní montáž zařízení s různou hmotností a rozměry.

Zámečnické konstrukce budou rovněž využity pro mobilní instalaci technologických komponent na vnější straně modulu, v souladu s požadavky na provozní flexibilitu a technickou kompatibilitu.

1.21 Bleskosvodná a uzemňovací soustava

Modul datového centra bude chráněn proti atmosférickým vlivům pomocí systému ochrany před bleskem (LPS – Lightning Protection System), který zajistí maximální bezpečnost zařízení a minimalizaci rizik pro osoby i majetek.
Na střeše modulu budou instalovány jímací tyče s možností snadné demontáže. Svody budou vedeny viditelně po obvodových stěnách modulu a každý svod bude vybaven zkušební svorkou pro kontrolu funkčnosti.

Pro uzemnění hromosvodu a silnoproudých zařízení bude zřízena uzemňovací soustava tvořená zemnícími tyčemi umístěnými kolem modulu. Ze zemničů budou vyvedeny spoje pro svody hromosvodu a hlavní ochrannou přípojnici. Veškeré kovové konstrukce v okolí modulu budou připojeny k této uzemňovací soustavě.

Uzemňovací soustava není součástí této veřejné zakázky a bude zajištěna samostatně Zadavatelem v rámci přípravy konkrétní lokality.

1.22 Servis mobilního datového centra

V místě instalace modulu datového centra bude k dispozici přívod pitné vody z veřejného vodovodního řadu, který může být využit pro servisní účely a případné budoucí napojení zvlhčovacích zařízení. Tento přívod však nebude přiveden přímo k modulu datového centra.

Odvod kondenzátu z chladicích a klimatizačních zařízení bude napojen na systém odvodnění instalační plochy tak, aby bylo zajištěno bezpečné odvádění vody a nedocházelo k jejímu vsakování do podloží nebo k poškození základové konstrukce.

Technologické řešení mobilního datového centra

1.23 Topologie infrastruktury

Infrastruktura mobilního datového centra musí splňovat požadavky pro úroveň **TIER III** dle klasifikace **Uptime Institute** nebo podle standardu **ANSI/TIA-942**. Systém musí být navržen tak, aby umožňoval servisovatelnost za plného provozu – všechny klíčové komponenty infrastruktury musí být vyměnitelné nebo opravitelné bez nutnosti odstávky IT systémů.

Hlavní požadavky na topologii infrastruktury zahrnují:

- **Plně redundantní napájecí systémy**, zajišťující nepřerušované napájení i při výpadku dodávky elektrické energie.
- **Redundantní chladicí systémy**, které udržují optimální provozní teplotu zařízení.
- **Redundance typu N+1** – každá kritická komponenta (napájení, chlazení) musí mít alespoň jednu záložní jednotku.
- Zajištění provozní kontinuity během údržby, díky použití redundantních prvků infrastruktury.
- Úroveň dostupnosti **minimálně 99,982 %**, což odpovídá maximálně přibližně 1,6 hodinám neplánovaného výpadku ročně.
- Průměrná roční hodnota PUE (Power Usage Effectiveness) nesmí překročit hodnotu **1,3**

1.24 Záložní zdroj elektrické energie

Zadavatel zajistí záložní zdroj elektrické energie formou motorgenerátoru odpovídajícího výkonu, který nebude součástí modulu kontejnerového datového centra. Napájení datového centra bude realizováno prostřednictvím dvou nezávislých napájecích větví, přičemž jedna z nich bude napájena přes motorgenerátor a bude sloužit jako primární (aktivní) větev. Druhá větev bude napojena přímo na externí transformátor a bude sloužit jako sekundární (pasivní) napájecí směr.

1.25 Elektrické napojení na místní zdroj elektrické energie

Redundantní napojení modulu datového centra na místní zdroj elektrické energie bude zajištěno provozovatelem prostřednictvím stávající infrastruktury, včetně dodávky napájecích kabelů.

Pro fyzickou ochranu kabelového vedení bude použita dvouplášťová chránička typu KOPOFLEX, určená pro zemní instalaci a dimenzovaná dle technických parametrů vedených kabelů. Chránička musí zajistit mechanickou ochranu, odolnost vůči vlhkosti a dlouhodobou provozní spolehlivost.

1.26 Dohledový kamerový systém

Pro zajištění vizuální kontroly, sledování provozu a identifikaci osob bude modul datového centra vybaven kamerovým systémem (CCTV). Kamery budou instalovány ve vnitřních i vnějších částech modulu, konkrétně:

- ve studené a teplé uličce,
- v podpůrné místnosti,
- prostor okolo kontejneru (všechny strany)

Použité kamery budou vybaveny pokročilou technologií s CMOS senzorem a vysokou světelnou citlivostí. Napájení kamer bude zajištěno prostřednictvím PoE (Power over Ethernet) switchů.
Záznam z kamer bude ukládán na záznamový server umístěný uvnitř modulu datového centra. Obsluha v dohledovém centru bude mít možnost vzdáleného přístupu k živému obrazu i

archivovaným záznamům, včetně možnosti vyhodnocení situací v reálném čase. On-line přenos bude umožněn i dohledu Odboru bezpečnosti a krizového řízeni (O30) Správy železnic.

1.27 Bezpečnostní technologie

Přístup do modulu datového centra bude chráněn prostřednictvím selektivního systému kontroly přístupu, který umožní autorizaci vstupu pouze oprávněným osobám. Součástí bezpečnostního řešení bude také ústředna poplachového zabezpečovacího a tísňového systému (PZTS), která zajistí dohled nad stavem zabezpečení objektu a umožní reakci na bezpečnostní incidenty.

Systém musí být navržen tak, aby splňoval požadavky na fyzickou bezpečnost, integraci s ostatními technologiemi modulu a umožňoval vzdálenou správu a monitoring. Systém musí být plně kompatibilní, integrovatelný a spravovaný stávajícím systémem ASSET Zadavatele.

1.27.1 Poplachový zabezpečovací a tísňový systém (PZTS)

Vnitřní prostory modulu datového centra budou chráněny pomocí duálních detektorů pohybu s antimaskingem (kombinace PIR + MW), které budou umístěny ve studené uličce, teplé uličce a podpůrné místnosti.

Všechny vstupní dveře, včetně dveří datových rozvaděčů a dveří oddělujících teplou a studenou uličku, budou vybaveny magnetickými kontakty pro detekci otevření.

Plášťová ochrana kontejneru bude realizována pomocí CCTV kamer s videoanalytickou funkcí a integrovány do stávajícího systému provozovaném zadavatelem.

Systém PZTS bude napojen na centrální monitorovací systém, který umožní sledování a vyhodnocování všech klíčových informací z bezpečnostních technologií a senzorů.

Při použití přístupové karty v kombinaci s číselným PIN kódem oprávněné osoby dojde k odblokování dveří a umožnění vstupu. Zastřežení a odstřežení systému bude prováděno prostřednictvím klávesnice umístěné ve vstupní chodbě. V případě narušení bude aktivován akustický alarm a informace o události bude předána do monitorovacího systému.

1.27.2 Systém elektronické kontroly vstupů (EKV)

Modul datového centra bude vybaven systémem elektronické kontroly vstupů (EKV), který zajistí řízený a bezpečný přístup do jednotlivých částí objektu. Systém bude tvořen bezkontaktními čtečkami karet s podsvícenou klávesnicí, biometrickými prvky a elektromechanickými zámky s bezpečnostními funkcemi.

Přístupový systém (EKV) bude integrovaný do centrálního bezpečnostního systému ASSET Zadavatele. Správu a řízení přístupu bude zastřešovat Odbor bezpečnosti a krizového řízeni (O30) Správy železnic.

Vstupní dveře do modulu (vnější plášť):

- Bezkontaktní čtečka karet s podsvícenou klávesnicí,
- Elektromechanický zámek s bezpečnostním kováním typu koule–klika (klika umístěna v chráněném prostoru) s funkcí anti-panik,
- Bezpečnostní cylindrická vložka,
- Minimálně čtyřbodové uzamčení typu EL566.
- Dveře budou osazeny samozavíračem (s kluznou lištou s možností otevření až 180°)
- Detektor nezavření dveří s opticko-zvukovou signalizací a napojením na EZS

Vstupní dveře do ICT sálu (vnitřní část):

- Bezkontaktní čtečka karet s podsvícenou klávesnicí,
- Elektromechanický zámek s bezpečnostním kováním typu koule–klika s funkcí anti-panik,
- Bezpečnostní cylindrická vložka,
- Čtyřbodové uzamčení typu EL566.
- Dveře budou osazeny samozavíračem (s kluznou lištou s možností otevření až 180°)
- Detektor nezavření dveří s opticko-zvukovou signalizací a napojením na EZS

Dveře do prostoru teplé uličky:

- Posuvné dveře s gravitačním zavíráním a s mechanickou aretací.

Dveře IT stojanů (datové rozvaděče):

- Bezkontaktní čtečka karet.

Všechny dveře (s výjimkou dveří datových rozvaděčů a dveří do teplé uličky) budou vybaveny elektromechanickým zámkem s funkcí anti-panik a budou splňovat požadavky bezpečnostní třídy **RC3 dle ČSN EN 1627**

1.28 Ochrana před požárem

Mobilní datové centrum bude vybaveno systémem elektrické požární signalizace (EPS) a samočinným hasicím zařízením (SHZ) na bázi chemického plynu. Systém SHZ bude navržen v souladu s normou **ČSN ISO 14520-1:2006**. Jako hasicí médium může být použito například NOVEC 1230.

Plynový SHZ bude konstruován tak, aby jeho funkčnost byla zachována i při úplném výpadku elektrické energie, včetně výpadku všech záložních zdrojů a akumulátorů.

Systém SHZ bude navržen bez nutnosti instalace přetlakových klapek pro odvod přetlaku/podtlaku při vypouštění hasiva do chráněného prostoru. Detekce požáru bude zajištěna kombinací opticko-kouřových detektorů a laserové nasávací detekce pro včasné odhalení požáru.

Ústředna SHZ bude napojena na monitorovací systém, který bude přijímat standardní signály:

- Porucha,
- Před-poplach,
- Poplach
- Hasivo vypuštěno.

V chráněném prostoru budou instalována tlačítka pro manuální spuštění a blokaci systému SHZ, doplněná o optickou a akustickou signalizaci.

1.28.1 Ochrana před požárem baterií UPS

Pro ochranu před požárem baterií UPS bude použity vhodné optické a ionizační detektory kouře, a senzory plamene v prostoru UPS.

SHZ pro baterie UPS bude konstruován tak, aby jeho funkčnost byla zachována i při úplném výpadku elektrické energie, včetně výpadku všech záložních zdrojů a akumulátorů.

Pro ochranu před požárem baterií UPS bude použit autonomní hasicí systém (např. Vermikulitový nebo F-500 systém) používající zónové hašení pouze v postižené části.

1.29 Systém chlazení a vzduchotechniky (VZT)

Mobilní datové centrum bude vybaveno kompletním systémem chlazení a vzduchotechniky, navrženým v souladu s požadavky úrovně **TIER III** dle Uptime Institute. Systém musí být plně servisovatelný za provozu a dimenzován pro chlazení IT vybavení s celkovou spotřebou **100 kW**.

Datové rozvaděče budou uspořádány tak, aby umožňovaly předozadní proudění vzduchu – klimatizovaný vzduch bude nasáván přední částí zařízení a teplý vzduch odváděn zadní částí. Pro zajištění účinného chlazení bude prostor teplé a studené uličky stavebně oddělen, čímž se zvýší efektivita systému.

Preferovaným řešením chlazení jsou **In-Row** klimatizační jednotky, umístěné v jedné řadě s racky a UPS v datové části modulu. Tyto jednotky budou pracovat s cirkulačním oběhovým vzduchem a budou vybaveny EC ventilátory pro snížení spotřeby elektrické energie.

Systém chlazení bude navržen s **N+1 redundancí**, přičemž potřebný výkon musí být pokryt 100 % chladicími jednotkami ve všech provozních režimech. Jednotky budou vybaveny integrovaným systémem řízení tlaku mezi teplou a studenou uličkou, který umožní přesné dávkování vzduchu dle aktuálních požadavků ICT zařízení.

Preferovaným řešením rozvodů pro distribuci chladiva jsou dva separované chladící okruhy vedené jinou trasou do davového sálu. Jako příklad možného řešení rozvodů pro distribuci chladiva může posloužit níže uvedený koncepční návrh zapojení chlazení serverovny (Ideologické schéma zapojení chlazení serverovny), který má sloužit jako podklad pro další technický návrh a neslouží jako závazný technický návrh.

Preferovanou technologií chlazení je CW systém, tedy kapalinové chlazení (voda/glykol).

Venkovní jednotky budou umístěny na střeše modulu a jejich konstrukce bude navržena tak, aby byly vizuálně integrovány do celkového vzhledu modulu a nebylo zřejmé, jaké technologie jsou uvnitř umístěny.

Systém chlazení bude dimenzován s ohledem na klimatické podmínky České republiky, včetně teplotních extrémů, vlhkosti a sezónních výkyvů. Vnitřní mikroklima bude řízeno dle požadavků ICT zařízení, přičemž doporučené teplotní a vlhkostní pásmo bude definováno podle standardu ASHRAE.

Systém musí umožňovat monitoring a regulaci teploty a vlhkosti v reálném čase, včetně generování alarmů při překročení limitních hodnot. Informace o ztrátě redundance nebo závadě systému budou předávány správě IT prostřednictvím e-mailu, SNMP trapu a webového rozhraní. Každá chladicí jednotka bude vybavena SNMP komunikační kartou, napojenou do monitorovacího systému.

Vnitřní i venkovní jednotky budou napájeny **ze dvou nezávislých zdrojů** s automatickým přepnutím v případě výpadku. Systém musí být navržen tak, aby umožňoval servisovatelnost za plného provozu – všechny klíčové komponenty chlazení musí být vyměnitelné nebo opravitelné bez nutnosti odstávky IT systémů.

Pro zvýšení bezpečnosti pracovníků uvnitř kontejneru, požadujeme v obou místnostech (Přechodová místnost i hlavní sál ITC) instalaci detektoru oxidu uhličitého - CO2 (monitor 'vydýchaného vzduchu') s LCD displejem pro přehled o úrovni CO2 v místnosti a akustickou signalizací pří překročení zdravotního limitu 1500ppm. Detektor musí být umístěn na dobře viditelném místě vedle dveří.

1.30 Systém napájení

Mobilní datové centrum bude vybaveno kompletním systémem elektrického napájení, který bude plně servisovatelný za provozu a navržen v souladu s požadavky úrovně **TIER III** dle Uptime Institute. Systém musí zajistit nepřetržité napájení všech ICT komponent, včetně záložních zdrojů a redundantních napájecích větví.

1.30.1 Napojení mobilního datového centra

Distribuce elektrické energie bude zahájena v nadřazené rozvodně, kde bude zajištěno napájení ze zálohované sítě prostřednictvím motorgenerátoru. Mobilní datové centrum bude napájeno prostřednictvím více napájecích větví, které zajistí provozní redundanci a vysokou dostupnost.

Systém napájení prioritně uvažuje s napojením z jednoho směru na úrovni 400V TN-C nebo TN-S vč. stacionárního zdroje el. energie – motorgenerátoru a zdroje nepřetržitého napájeni na úrovni 230/400VAC. Provedení rozvaděčů musí umožňovat připojení systému datového centra také z druhého napájecího směru, včetně mobilního motorgenerátoru. Motorgenerátor není součástí tohoto projektu.

Součástí projektu je ovšem realizace přípojného bodu pro napojení kabelu z druhého napájecího směru a přípojného bodu pro napojení mobilního motorgenerátoru.

Napájecí infrastruktura musí být navržena tak, aby umožňovala bezpečný provoz, snadnou údržbu a rozšíření v budoucnosti. Všechny komponenty musí být kompatibilní s požadavky na provozní spolehlivost a energetickou účinnost.

1.30.2 Distribuce elektrické energie

Distribuce elektrické energie musí dodržovat topologii dvojitého napájení (větev A / větev B) pro všechny spotřebiče v datovém centru. Z hlediska dostupnosti elektrického napájení budou spotřebiče v mobilním datovém centru rozděleny do následujících kategorií:

- Zálohovaná zařízení (napájená ze záložních zdrojů UPS)
  - Datové rozvaděče
  - Servery
  - Datová uložiště
  - Síťová infrastruktura (switche, routery, firewally)
  - Řídicí systémy chlazení (např. řídicí jednotky klimatizací)
  - Bezpečnostní systémy (např. přístupové systémy, CCTV)
  - Ovládání motorgenerátoru (startovací logika, palivové čerpadlo)
  - Osvětlení nouzových zón (např. datový sál, podpůrná místnost)
- Nezálohovaná zařízení (napájené napřímo, bez podpory UPS, zálohované motorgenerátorem)
  - Celý IT provoz (včetně toho, co je na UPS)
  - Chladicí systémy (CRAC jednotky, chillery)
  - Osvětlení celého objektu
  - Zabezpečovací systémy modulu
  - Nabíjení baterií UPS

Jako příklad možného řešení rozvodů pro napájení datového centra může posloužit níže uvedený koncepční návrh zapojení napájení serverovny (Ideologické schéma zapojení napájení serverovny), který má sloužit jako podklad pro další technický návrh a neslouží jako závazný technický návrh.

Distribuce elektrické energie pro kontejnerového datové centrum bude zajištěna prostřednictvím **dvou nezávislých napájecích větví**, které budou navzájem redundantní:

- **Větev A (primární/aktivní)** bude napájena z externího transformátoru přes **motorgenerátor**, který bude v běžném provozu aktivní a bude sloužit jako hlavní zdroj napájení
- **Větev B (sekundární/pasivní)** bude napojena přímo na externí transformátor bez motorgenerátoru. Tato větev bude sloužit jako záložní napájecí směr. V případě potřeby bude možné k této větvi připojit **mobilní motorgenerátor**.

Obě napájecí větve budou zakončeny samostatnými rozvaděči, které budou zajišťovat distribuci elektrické energie pro technologické systémy, včetně chlazení a záložních zdrojů UPS.

V případě výpadku primární napájecí větve bude automaticky spuštěn motorgenerátor, který převezme funkci hlavního zdroje elektrické energie pro datové centrum. **Sekundární větev** umožňuje připojení **mobilního motorgenerátoru** pro případ výpadku napájení i na této trase.

Zálohované napájení ICT infrastruktury bude zajištěno prostřednictvím **dvou samostatných rozvaděčů RUPS-A a RUPS-B**, které budou připojeny k oběma napájecím větvím. Tím bude zajištěna redundance a vysoká dostupnost napájení.

- Zálohovaná ICT infrastruktura bude napájena přes **systém UPS**, který zajistí nepřerušené napájení v případě výpadku obou napájecích větví, po dobu nutnou k náběhu motorgenerátoru.
- Po spuštění motorgenerátoru bude napájení automaticky přepnuto na generovaný zdroj.

Nezálohovaná ICT infrastruktura bude napájena přímo z napájecích rozvaděčů bez použití UPS. V případě výpadku napájení bude jejich provoz obnoven po spuštění motorgenerátoru.

Pasivní napájecí větev bude také sloužit k napájení technologií během servisních zásahů na aktivní větvi, čímž bude zajištěna provozní kontinuita.

Všechny kovové části zařízení a vedení uvnitř modulu budou vodivě propojeny do jednotné zemnící sítě, která bude vyvedena vně modulu a připojena na vnější uzemňovací síť objektu. Uzemnění bude provedeno v souladu s normou **ČSN EN 50310 ed.4**.

Pro ochranné pospojování budou ve všech technických místnostech instalovány hlavní ochranné přípojnice (HOP), ke kterým budou připojeny všechny velké kovové hmoty v dosahu – včetně rozvaděčů, zařízení VZT, klimatizací, kovových konstrukcí, ústředen SLP apod. Tyto přípojnice budou propojeny s vnější uzemňovací sítí objektu, která není součástí této veřejné zakázky. Modul bude vybaven svorkami pro jednoduché připojení k této síti.

Součástí systému napájení bude ochrana proti přepětí, realizovaná vhodnou instalací přepěťových ochran v napájecí síti.

Pro případ dlouhodobé odstávky primárního napájení nebo fatální poruchy bude modulární datové centrum vybaveno přívodem pro napájení z mobilního motorgenerátoru, napojeným do pasivní napájecí větve.

Celá distribuční soustava bude monitorována, včetně stavu jistících a spínacích prvků. Měření spotřeby a sledování parametrů sítě bude přenášeno do monitorovacího systému, který umožní vyhodnocování provozních dat, včetně výpočtu PUE datového centra.

1.30.3 Zdroj nepřerušitelného napájení (UPS)

Mobilní datové centrum bude vybaveno kompletním systémem zdrojů nepřerušitelného napájení, který bude navržený v souladu s požadavky úrovně **TIER III** dle Uptime Institute. Systém musí být plně servisovatelný za provozu a dimenzován pro zajištění nepřerušitelného napájení ICT infrastruktury, řídicího systému chlazení a systému monitoringu. Budou instalovány **dva modulární UPS systémy**, každý o výkonu **minimálně 100 kW.** Přičemž výkonové moduly napájecího systému budou dimenzovány v konfiguraci minimálně N+1.

Každý UPS systém bude tvořen výkonovými moduly o výkonu **min. 20 kVA / 20 kW**, které budou:

- uživatelsky vyměnitelné („hot-swappable"),
- instalovatelné za provozu bez přerušení napájení,
- vybavené integrovaným statickým přepínačem (static switch),
- vybavené samostatným řídicím systémem.

Pro zajištění nepřerušeného provozu během startu motorgenerátoru bude každý UPS systém vybaven vlastní bateriovou sadou.

Požadovaná doba zálohování je **minimálně 10 minut při plné zátěži 100 kW** a provozu všech modulů a bateriových sad.

UPS systémy musí být schopny informovat správu IT o:

- ztrátě redundance,
- poruše nebo výpadku modulu,

prostřednictvím:

- e-mailu,
- SNMP trapu,
- webového rozhraní.

Komunikační SNMP karta bude součástí zařízení a napojena do systému monitoringu.

1.30.4 Základní požadavky na zdroje UPS

UPS systémy musí splňovat následující technické požadavky:

- **Modulární architektura DPA** (Decentralized Parallel Architecture) – paralelní zapojení výkonových modulů o min. výkonu 20 kVA / 20 kW
- **Hot-swappable moduly** – výměna a instalace za provozu bez nutnosti zásahu specializovaného technika
- Baterie typu **$LiFePO_4$** (Lithium Iron Phosphate) s dlouhou životností, s nízkými nároky na údržbu, kompaktními rozměry, vhodné pro aplikace s vysokou dynamikou zátěže
- Každý modul musí obsahovat:
  - vlastní statický přepínač (static switch),
  - samostatný usměrňovač,
  - nezávislý řídicí systém,
  - LCD displej pro ovládání, monitoring a správu provozních parametrů
- Vysoká účinnost v on-line režimu s dvojitou konverzí
- Minimální efektivita **95,5 %** při zatížení 50–75 % nominálního výkonu při provozu ze sítě.
- Integrovaný manuální servisní bypass – umožňuje přesměrování napájení mimo UPS pro účely údržby bez přerušení dodávky energie

- Senzor pro teplotně kompenzované dobíjení – optimalizace nabíjecího napětí dle aktuální teploty baterií
- Rozhraní pro výstup do systému měření a regulace (MaR) – prostřednictvím SNMP protokolu a reléových kontaktů.

1.30.5 Osvětlení

Řešení provozního osvětlení bude navrženo s ohledem na členění prostor dle architektonických, provozních a hygienických požadavků. Osvětlení bude realizováno v souladu s normou **ČSN EN 12464-1**, tak aby byly splněny požadované hodnoty osvětlenosti v jednotlivých rovinách a prostorách, a zároveň byla zajištěna maximální světelná pohoda.

Použita budou **energeticky úsporná LED svítidla**, s odpovídajícím krytím dle charakteru prostoru.

Napájení osvětlení bude rozděleno rovnoměrně:

- 50 % z rozváděče RUPS-A
- 50 % z rozváděče RUPS-B

Požadované minimální hodnoty osvětlenosti dle ČSN:

- Technické prostory, strojovny – min. 200 lx
- Místnost s datovými rozvaděči – min. 500 lx

Ovládání svítidel bude realizováno místními vypínači umístěnými u dveří jednotlivých místností.

1.30.6 Venkovní osvětlení

Venkovní osvětlení bude zajištěno pomocí minimálně 4 ks LED reflektorů, umístěných na mobilních konzolách na střeše kontejneru. Ovládání reflektorů bude:

- Manuální
- Automatické – na základě signálu z minimálně 4 ks pohybových čidel umístěných v exteriéru nebo na základě analytických funkcí venkovních kamer.

1.30.7 Nouzové osvětlení

Nouzové osvětlení bude navrženo tak, aby:

- jasně a jednoznačně vyznačovalo únikové cesty,
- zajistilo viditelnost překážek a bezpečný přesun osob k nouzovým východům,
- označovalo poplachová, protipožární a důležitá ovládací zařízení.

Požadované hodnoty osvětlenosti dle **ČSN EN 1838**:

- Únikové cesty – min. 1 lx v osách
- Požárně bezpečnostní zařízení mimo únikové cesty – min. 5 lx

Nouzové osvětlení bude realizováno pomocí LED svítidel s integrovanou baterií, s předpokládanou dobou provozu v nouzovém režimu **min. 1 hodinu**.

ITC řešení mobilního datového centra

1.31 Mobilní datacentrový modul

Mobilní datové centrum je navrženo jako trvale bezobslužné pracoviště, bez stálé fyzické obsluhy. Představuje řešení pro uživatele s požadavky na:

- rychlou výstavbu,
- mobilitu,
- kompaktní prostorové nároky.

Veškerá infrastruktura datového centra je integrována do **jednoho modulárního kontejneru**, který obsahuje:

- všechna ICT zařízení,
- podpůrné technologie nutné pro provoz.

1.31.1 Členění modulu

Modul je rozdělen do dvou hlavních funkčních částí:

- Podpůrná místnost (vstupní komora),
- Datový sál s ICT zařízeními.

1.31.2 Podpůrná místnost

Podpůrná místnost plní funkci vstupní komory, která je konstrukčně oddělena od venkovního prostředí. Slouží jako ochranná bariéra proti vniknutí vody, prachu a dalších nečistot. Z této komory je zajištěn kontrolovaný přístup do prostoru s ICT technologiemi.

Současně tato místnost slouží jako přechodový prostor mezi exteriérem a datovým sálem, příruční sklad a místo pro instalaci vybraných technologických zařízení (např. elektrických rozvaděčů). Tímto uspořádáním se omezuje nutnost vstupu obslužného a servisního personálu přímo do datového sálu mobilního datového centra, čímž se zvyšuje bezpečnost a provozní efektivita.

1.31.3 Datový sál

V datovém sále budou instalovány datové rozvaděče (racky) dle průmyslového standardu **19''**, určené pro běžný IT hardware třetích stran. Proudění vzduchu bude řešeno z přední části do zadní, s cílem optimalizace chlazení.
Rozmístění rozvaděčů bude navrženo tak, aby vznikla oddělená ulička pro rozdělení chladného a ohřátého vzduchu. Součástí bude:

- 1 vstupní dveře do studené nebo teplé uličky,
- Každý rozvaděč bude vybaven zamykacími jednodílnými dveřmi v přední části a dělenými dveřmi v zadní části.

1.32 Datové rozvaděče

Pro instalaci IT technologií bude dodáno **minimálně 8 ks datových rozvaděčů (racků)** typu **19"**, každý o rozměrech:

- šířka: 800 mm,
- hloubka: min. 1200 mm,
- výška: 42U.

Rozvaděče budou mít stabilní rámovou konstrukci s nosností **min. 1300 kg** (dynamické zatížení). Ukotvení rozvaděčů bude provedeno do rámu kontejneru s ponecháním mezer mezi stojany, čímž vznikne prostor pro:

- kabeláž,
- PDU lišty,
- vyvazovací příslušenství.

Rozmístění rozvaděčů musí umožnit:

- bezproblémovou instalaci zařízení ze strany studené uličky,
- podporu montáže zařízení s různou hloubkou.

Součástí dodávky budou:

- záslepky pro uzavření min. **80 %** volných U pozic, v provedení pro bez nástrojovou montáž,
- separační rám pro oddělení teplé a studené uličky,
- šrouby a klecové matice pro uchycení zaslepovacích panelů.

1.32.1 PDU lišty

Každý datový rozvaděč bude vybaven **minimálně** čtyřma **vertikálními měřenými PDU lištami** se zásuvkami **C13 a C19**, které:

- nezasahují do U pozic,
- nebrání instalaci kabeláže ani hlubokých IT zařízení,
- budou vnořeny do rámu skříně a instalovány na zadní straně rámu.
- Dvě třífázové PDU (32 A) ve spodní části racku:
    - Minimálně 8x C19 zásuvek a minimálně 8x C13 zásuvek
- Dvě jednofázové PDU (16 A) v horní části racku:
    - Minim
    - lně 4x C19 zásuvek a minimálně 12x C13 zásuvek

Napájení PDU lišt:

- dvě lišty z napájecí větve A
- dvě lišty z napájecí větve B

PDU lišty budou **měřené a monitorované**, musí obsahovat dostatečný počet zásuvek pro připojení všech ICT zařízení v plně osazeném racku, napojené do systému monitoringu pro účely sledování:

- spotřeby elektrické energie,
- výpočtu PUE datového centra.

1.32.2 Senzory

Do PDU lišt budou integrována teplotně-vlhkostní čidla:

- 4 ks ve studené uličce,
- 2 ks v teplé uličce

Každé čidlo bude připojeno **samostatně do jedné PDU lišty**.

1.32.3 Přístupový systém

Každý datový rozvaděč bude vybaven samostatným elektronickým kartovým přístupovým systémem, který bude integrovaný do centrálního bezpečnostního systému ASSET Zadavatele. Správu a řízení přístupu bude zastřešovat Odbor bezpečnosti a krizového řízeni (O30) Správy železnic.

1.33 Strukturovaná kabeláž

Součástí dodávky mobilního datového centra bude předkonektorovaná strukturovaná kabeláž, zahrnující:

- **optickou infrastrukturu**
  - OM4, MM, Duplex, SC/UPC
  - OS2, SM, Simplex, E2000/APC
- **metalickou infrastrukturu** (kategorie CAT6a).
- Optické a metalické datové kabely požadujeme oddělit do vlastních kabelových žlabů (každý typ kabelu do vlastního žlabu)

1.33.1 Racková výbava

Každý serverový rozvaděč (rack) bude standardně osazen:

- 1 patch panelem s minimálně:
  - **12** optickými porty typu LC duplex (OM4)
  - **6** metalickými porty kategorie CAT6a.

1.33.2 LAN rozvaděč

Jeden z datových rozvaděčů bude vyhrazen jako LAN datový rozvaděč pro:

- ukončení síťové konektivity,
- správu datové infrastruktury.

V tomto rozvaděči budou instalovány:

- odpovídající počet 1U panelů pro zakončení na optických a metalických kazetách.

1.33.3 Rozšiřitelnost

Patch panely musí obsahovat volné pozice pro budoucí rozšíření datové infrastruktury.

1.34 Monitorovací a řídicí systém

Pro potřeby sledování a řízení funkcionality podpůrné infrastruktury mobilního datového centra musí být instalován monitorovací a řídící systém, který bude sledovat parametry a události v reálném čase. Monitorovací a řídící systém musí shromažďovat, analyzovat, zpracovávat, integrovat, vyhodnocovat trendy ve všech kritických parametrech Non-IT infrastruktury a pomáhat tak udržet nejvyšší možnou dostupnost datového centra.

Systém monitoringu bude sloužit pro monitorování kompletní infrastruktury mobilního datového centra a bude koncipován jako autonomní ucelený.

Monitorovací systém musí zajišťovat dohled nad všemi Non-IT technologiemi a prostředím vybraných prostor. Sběr dat z jednotlivých technologií bude realizován prostřednictvím komunikačních protokolů přímo monitorovacím systémem. Veškeré informace z technologií, senzorů a chladicích jednotek budou načítány pomocí PLC jednotky, která bude umístěna v samostatném rozvaděči. PLC musí obsahovat algoritmy pro vyhodnocování alarmových stavů,

trvalé ukládání logů událostí a uchovávání trendových dat na lokálním úložišti (např. SD karta) v případě nedostupnosti centrální části systému. Návrh kabelových tras včetně použitých kabelů bude v kompetenci zhotovitele, který musí zajistit plnou kompatibilitu s dodávaným systémem a garantovat požadovanou funkcionalitu.

Monitorovací systém musí zajišťovat sběr a sledování následujících parametrů:

- **Komunikace s technologiemi:** Sběr dat ze všech monitorovaných zařízení a technologických celků musí být realizován prostřednictvím komunikačních rozhraní integrovaných v jednotlivých technologiích nebo jejich nadřazených řídicích systémech
- **Napájecí systém:** Monitoring musí zahrnovat dohled nad zdroji UPS, řídicím systémem energetiky, polohou všech jistících a spínacích prvků, měřením odběru a spotřeby elektrické energie na vstupu do datového centra i pro napájení IT technologií. Dále musí být sledovány elektrické veličiny (napětí, proud, výkon, účiník) samostatně pro každý rozvaděč
- **Chladicí systém:** Systém musí umožňovat datovou komunikaci se všemi chladicími jednotkami a jejich nadřazeným řídicím systémem
- **Fyzická bezpečnost:** Monitoring musí zahrnovat systémy SHZ (stabilní hasicí zařízení), EZS (elektronický zabezpečovací systém) a EKV (elektronická kontrola vstupu)
- **Prostředí datové a energetické části:** Sledování teploty a relativní vlhkosti musí být zajištěno jak ve studené, tak v teplé zóně datové části, stejně jako v energetické části
- **Detekce úniku kapalin:** Systém musí monitorovat případné úniky kapalin ve všech relevantních místnostech

Monitorovací systém musí umožňovat archivaci událostí a trendových hodnot všech sledovaných parametrů tak, aby byly efektivně dostupné pro další uživatele nebo systémy (např. pro integraci do nadřazených systémů nebo pro reporting v rámci SLA). Systém musí rovněž podporovat evidenci externích informací vzniklých mimo vlastní monitorovací infrastrukturu, jako jsou:

- Reakce obsluhy na incidenty,
- Konfigurace prahových hodnot pro alarmový systém,
- Parametry automaticky prováděných eskalačních procesů,
- Související evidenční databáze.

Součástí databáze musí být také správa přístupových oprávnění jednotlivých uživatelů systému.

Monitorovací systém musí splňovat následující funkční požadavky:

- **Centrální zpracování dat**: Veškeré informace musí být zpracovávány v centrální serverové části systému. Ta musí zajišťovat vyhodnocování dat v reálném čase, jejich archivaci po dobu minimálně 18 měsíců a eskalaci vzniklých událostí dle definovaného schématu.
- **Vizualizace provozních ukazatelů:** Systém musí umožňovat vizualizaci klíčových provozních hodnot, jako je ukazatel PUE (Power Usage Effectiveness), aktuální doba autonomie baterií UPS a další relevantní parametry.
- **Zobrazení pro různé typy uživatelů:** Rozhraní musí být optimalizováno pro zobrazení na monitorech s rozlišením FullHD pro operátory, a zároveň musí být dostupné pro vzdálené uživatele prostřednictvím standardního webového rozhraní nebo mobilní aplikace.
- **Definice odvozených alarmů:** Systém musí umožňovat uživatelskou konfiguraci odvozených alarmů na základě primárních alarmových stavů, jejich limitních hodnot a provozních podmínek.

- **Eskalace alertů:** Musí být zajištěna spolehlivá eskalace výstrah prostřednictvím SMS zpráv, a to bez závislosti na externí infrastruktuře – pomocí GSM modemu integrovaného přímo do jádra systému
- **Integrace s nadřazeným systémem:** Systém musí být schopen předávat data prostřednictvím API do nadřazeného monitorovacího systému Zadavatele, založeného na platformě ZABBIX. A zároveň musí poskytnout možnost napojení na systém dálkové diagnostiky DDTS provozovaného Zadavatelem.
- **Lokální server:** Lokální dohledový server musí být fyzicky umístěn v mobilním datovém centru.
- **Webový přístup:** Po zprovoznění komunikační trasy a konfiguraci musí být výstupy z monitorovacího systému okamžitě dostupné prostřednictvím zabezpečeného webového rozhraní (HTTPS) z libovolného PC vybaveného webovým prohlížečem

1.34.1 Požadavky na uživatelské rozhraní systému

Monitorovací systém musí být vybaven webovým rozhraním určeným pro práci operátorů a dalších oprávněných uživatelů. Rozhraní musí být dostupné z libovolného počítače s připojením k serveru monitorovacího systému. Navigace mezi jednotlivými schématy a detaily technologií musí být intuitivní, s využitím hypertextových odkazů pro přechod mezi zobrazeními.

Jako příklad možného řešení vizualizace monitorovaného prostředí datového centra a aktuálního stavu prostředí datového centra může posloužit níže uvedený koncepční návrh (Ideologické schéma vizualizace monitorovaného prostředí serverovny), který má sloužit jako podklad pro další technický návrh a neslouží jako závazný technický návrh.

Rozhraní musí dále poskytovat následující funkce:

- **Grafické zobrazení průběhu teploty a vlhkosti** na jednotlivých senzorech, včetně vyznačení časových intervalů, kdy byly překročeny nastavené mezní hodnoty. Uživatelé s příslušným oprávněním musí mít možnost tyto meze upravovat.
- **Grafické zobrazení průběhu sledovaných elektrických veličin**, jako jsou napětí, proud, výkon apod.
- **Seznam událostí** s rozlišením jejich závažnosti a aktuálního stavu, včetně detailního zobrazení jednotlivých událostí a souvisejících systémových i uživatelských aktivit.
- **Monitoring polohy vývodových jističů**, včetně možnosti uživatelského popisu jednotlivých vývodů.

Bez ohledu na aktuálně zobrazený detail musí být vždy dostupný seznam aktivních poplachů, který bude obsahovat čas vzniku a ukončení poplachu, čas potvrzení obsluhou, počet opakování a popis události. Seznam musí umožňovat přímý přechod na zobrazení technologie, která poplach vyvolala, na detail události a (v případě odpovídajícího oprávnění) potvrzení jednotlivých nebo všech nevyřešených poplachů.

Systém nesmí omezovat počet vytvořených uživatelských účtů ani počet současně připojených uživatelů z hlediska licencování.

Uživatelské rozhraní musí podporovat vícejazyčné zobrazení, minimálně v českém a anglickém jazyce, s možností nastavení preferovaného jazyka individuálně pro každého přihlášeného uživatele.

Systém musí umožnit jednotlivým uživatelům nastavení nebo deaktivaci akustické signalizace aktivních událostí, s výjimkou uživatelů s rolí operátora, u nichž musí být signalizace trvale aktivní.

Správa uživatelských účtů a přidělování oprávnění bude plně v kompetenci Zadavatele. Systém musí umožňovat definici a správu minimálně následujících uživatelských rolí:

- **Běžný uživatel**: Přístup k systému a zobrazení všech nebo vybraných informací dle přiděleného kontextu. Možnost přístupu k logům událostí a reportům. Umožnění zápisu komentářů k událostem a na evidenční karty jednotlivých technologií.
- **Operátor**: Oprávnění pro práci s alarmy a evidencí technologií v rámci odpovědnosti za provoz a reakci na vzniklé události.
- **Správce provozu**: Oprávnění ke konfiguraci provozních parametrů, včetně nastavení limitních hodnot pro vyhlašování událostí, definice alarmů druhé úrovně na základě primárních alarmů nebo kombinace provozních podmínek, a blokování alarmů pro odstavené technologie.
- **Správce systému**: Oprávnění pro globální správu uživatelů, konfiguraci systémových parametrů, zálohování dat, provádění off-line operací a další systémové činnosti.

Profylaktické kontroly a revize mobilního datového centra

Dodavatel je povinen zajistit pravidelnou provozní kontrolu a revize podpůrných systémů mobilního datového centra v souladu s technickými specifikacemi výrobce. Kontrola bude prováděna kvalifikovaným servisním nebo revizním technikem podle specifikace a požadavků v podkapitolách níže. Cílem kontroly a revize je ověření provozuschopnosti systému, jeho souladu s definovanými technickými parametry, specifikacemi výrobce, s platnými právními předpisy a technickými normami.

Dodavatel je povinen zajistit pravidelnou provozní kontrolu a revize podpůrných systémů mobilního datového centra **po dobu 10 let** od předání a zprovoznění mobilního datového centra Zadavateli.

Dodavatel je povinen zajistit provozuschopnost mobilního datového centra a jeho kritických i nekritických prvků po dobu 10 let.

1.35 Profylaktické kontroly a revize zdroje nepřetržitého napájení (UPS)

Dodavatel je povinen zajistit pravidelnou provozní kontrolu a revizi UPS systému v souladu s technickými specifikacemi výrobce. Kontrola bude prováděna **1× ročně** kvalifikovaným servisním technikem. Cílem kontroly je ověření provozuschopnosti systému, jeho souladu s definovanými technickými parametry a podmínkami prostředí.

Rozsah provozní kontrola UPS (1x ročně):

- Ověření souladu provozního prostředí UPS s definovanými podmínkami
- Kontrola funkčnosti ventilátorů a proudění vzduchu
- Analýza registru událostí UPS na výskyt alarmových stavů
- Kontrola výkonových svorek UPS pod zátěží
- Kontrola zbývajících svorek, které nebyly zahrnuty v předchozím kroku
- Bodové měření teploty svorek interních a/nebo externích baterií
- Termovizní měření teploty výkonových svorek a komponent UPS
- Porovnání skutečných hodnot napětí a proudu s údaji na displeji (je-li k dispozici)
- Provedení testu vybíjení
- Ověření funkce přepnutí na bateriový provoz
- Test funkčnosti interního statického bypassu
- Vyčištění UPS od prachu a nečistot
- Kontrola kondenzátorových bank (je-li součástí systému)
- Vizuální a funkční kontrola vnitřních řídicích a výkonových vodičů
- Kontrola dotažení výkonových přípojek uvnitř UPS
- Vizuální kontrola externích bateriových systémů (je-li tak zařízení vybaveno)
- Ověření aktuální verze firmware a případná aktualizace
- Měření izolačního odporu v rámci pravidelné elektrorevize

Rozsah provozní kontroly bateriového systému (1x ročně):

- Vizuální kontrola zapojení baterií
- Test impedance/vodivosti baterií a vybíjení
- Měření teploty svorek baterií, zvlnění AC napětí a proudu
- Dotažení svorek dle specifikace výrobce
- Kontrola výskytu koroze nebo úniku elektrolytu, včetně vyčištění systému

- Poskytnutí doporučení k výměně baterií, pokud jsou mimo toleranční hodnoty

1.36 Profylaktické kontroly a revize elektrozařízení

Dodavatel je povinen zajistit pravidelné revize všech elektrozařízení instalovaných v prostoru serverovny. Součástí této povinnosti je vedení kompletní dokumentační agendy revizních úkonů pro každé jednotlivé zařízení. **Revize** musí být prováděny v souladu s platnými právními předpisy, technickými normami a specifikacemi výrobce.

1.36.1 Provozní kontrola jednotek PDU (Power Distribution Unit)

Servisní technik provede vizuální a elektronickou kontrolu jednotek PDU za účelem ověření jejich provozuschopnosti a souladu s technickými specifikacemi a podmínkami prostředí.

Rozsah provozní kontroly PDU (1x ročně):

- Ověření souladu provozního prostředí s definovanými podmínkami
- Kontrola registru událostí PDU na výskyt alarmových stavů
- Kontrola výkonových svorek pod zátěží
- Kontrola zbývajících svorek, které nebyly zahrnuty v předchozím kroku
- Termovizní měření teploty svorek (včetně pořízení snímku)
- Porovnání skutečných hodnot napětí a proudu s údaji na displeji (je-li k dispozici)
- Vyčištění jednotky od prachu a nečistot
- Vizuální kontrola vnitřních vodičů (řídicích i výkonových)
- Kontrola dotažení výkonových přípojek
- Ověření verze firmware a případná aktualizace
- Měření izolačního odporu v rámci elektrorevize
- Zápis zjištěných stavů do revizní dokumentace

1.36.2 Provozní kontrola rozváděčů RUPSA a RUPSB

Servisní technik provede vizuální a funkční kontrolu rozváděčů RUPS za účelem ověření jejich provozuschopnosti a souladu s technickými specifikacemi.

Rozsah provozní kontroly rozvaděčů (1x ročně):

- Ověření souladu provozního prostředí s definovanými podmínkami
- Kontrola registru událostí řídicího systému
- Kontrola výkonových svorek pod zátěží
- Kontrola zbývajících svorek, které nebyly zahrnuty v předchozím kroku
- Termovizní měření teploty svorek (včetně pořízení snímku)
- Porovnání skutečných hodnot napětí a proudu s údaji na displeji (je-li k dispozici)
- Vyčištění rozváděče od prachu a nečistot
- Vizuální kontrola vnitřních vodičů
- Kontrola dotažení výkonových přípojek
- Ověření verze firmware a případná aktualizace
- Kontrola a měření baterií záložního zdroje
- Měření izolačního odporu v rámci elektrorevize
- Zápis zjištěných stavů do revizní dokumentace

1.36.3 Provozní kontrola ATS

Servisní technik provede vizuální a funkční kontrolu ATS rozváděče.

Rozsah provozní kontroly ATS (1x ročně):

- Ověření souladu provozního prostředí s definovanými podmínkami
- Kontrola registru událostí řídicího systému ATS
- Kontrola výkonových svorek pod zátěží
- Kontrola zbývajících svorek, které nebyly zahrnuty v předchozím kroku
- Termovizní měření teploty svorek (včetně pořízení snímku)
- Porovnání skutečných hodnot napětí a proudu s údaji na displeji (je-li k dispozici)
- Vyčištění rozváděče od prachu a nečistot
- Vizuální kontrola vnitřních vodičů
- Kontrola dotažení výkonových přípojek
- Ověření verze firmware a případná aktualizace
- Kontrola a měření baterií záložního zdroje
- Měření izolačního odporu v rámci elektrorevize
- Zápis zjištěných stavů do revizní dokumentace

1.37 Profylaktické kontroly a revize jednotek chlazení

Dodavatel je povinen zajistit pravidelnou vizuální a funkční kontrolu klimatizačního systému, a to včetně vnitřních i venkovních jednotek. Cílem kontroly je ověření provozuschopnosti systému, jeho souladu s technickými specifikacemi výrobce a podmínkami prostředí. Kontrola musí být prováděna kvalifikovaným servisním technikem.

Rozsah provozní kontroly vnitřních klimatizačních jednotek (1x ročně):

- Ověření souladu provozního prostředí (prach, vlhkost, vibrace) s definovanými podmínkami
- Vizuální kontrola zařízení (poškození, opotřebení, nestandardní úpravy)
- Kontrola výkonových svorek pod zátěží (včetně krytů a úchytů)
- Kontrola chodu ventilátorů (hlučnost, doběh, rozběh)
- Kontrola otáček ventilátorů
- Kontrola mechanických částí motoru a dotažení spojů
- Kontrola čistoty lamel výměníku a průchodnosti vzduchu
- Kontrola odvzdušnění a těsnosti chladicího okruhu
- Kontrola úkapů a čistoty okolí jednotky
- Kontrola odvodu kondenzátu (je-li zařízení vybaveno)
- Kontrola, vyčištění a výměna vzduchového filtru (výměna 1× ročně)
- Kontrola funkce termostatu (nastavení a odezva systému)
- Kontrola funkce termického pohonu (je-li součástí)
- Kontrola stavové signalizace (logy, chybové hlášení, servisní intervaly)
- Kontrola registru událostí řídicího systému (je-li zařízení vybaveno)
- Měření teploty svorek pomocí termokamery nebo bezdotykového teploměru
- Porovnání skutečných hodnot napětí a proudu s údaji na displeji (je-li k dispozici)
- Vyčištění pomocných rozváděčů klimatizace (je-li součástí)
- Ověření verze firmware a případná aktualizace (je-li zařízení vybaveno)

Rozsah provozní kontroly venkovních klimatizačních jednotek (1x ročně):

- Ověření souladu provozního prostředí (prach, vlhkost, vibrace) s definovanými podmínkami
- Vizuální kontrola zařízení (poškození, opotřebení, nestandardní úpravy)
- Kontrola výkonových svorek pod zátěží (včetně krytů a úchytů)
- Kontrola chodu ventilátorů (hlučnost, doběh, rozběh)
- Kontrola otáček ventilátorů
- Mytí výměníku tlakovou vodou (min. 1× ročně)

- Kontrola mechanických částí motoru a dotažení spojů
- Kontrola čistoty lamel výměníku a průchodnosti vzduchu
- Kontrola odvzdušnění a těsnosti chladicího okruhu
- Kontrola úkapů a čistoty okolí jednotky
- Kontrola odvodu kondenzátu (je-li zařízení vybaveno)
- Kontrola kompresorové jednotky a jejího opotřebení

1.38 Profylaktické kontroly a revize monitorovacího systému

Dodavatel je povinen zajistit pravidelnou vizuální a funkční kontrolu systému monitoringu prostředí, včetně hardwarových i softwarových komponent. Cílem kontroly je ověření provozuschopnosti systému, jeho souladu s technickými specifikacemi výrobce a podmínkami prostředí. Kontrola musí být prováděna kvalifikovaným servisním technikem.

Rozsah provozní kontroly hardwarových komponent systému monitoringu (1x ročně):

- Kontrola funkčnosti čidel (teplotních, vlhkostních, záplavových)
- Ověření komunikace všech jednotek
- Kontrola komunikačních propojení
- Ověření aktuálnosti firmware komunikačních zařízení a případná aktualizace
- Kontrola funkčnosti kamerového systému monitoringu prostředí
- Kontrola spojů a všech signalizačních kontaktů
- Kontrola měření, komunikace a zatížení systému
- Úprava uživatelského nastavení systému monitoringu

Rozsah provozní kontroly softwarových komponent systému monitoringu (1x ročně):

- Ověření komunikace všech jednotek – dostupnost a funkčnost monitorovaných zařízení
- Kontrola správnosti údajů ze senzorů (teplota, vlhkost, záplavy)
- Kontrola správného označení a nastavení provozních parametrů
- Kontrola uložených dat a jejich interpretace
- Záloha nastavení a uložených dat
- Kontrola správného nastavení data a času
- Ověření aktuálnosti softwarové verze a případná aktualizace
- Kontrola funkčnosti kamerového systému monitoringu prostředí
- Ověření aktivace a hlášení alarmových stavů
- Kontrola spojů a všech signalizačních kontaktů
- Ověření aktuálnosti firmware monitorovaných zařízení a případná aktualizace

1.39 Profylaktické kontroly a revize stabilního hasicího zařízení (SHZ)

Dodavatel je povinen zajistit pravidelnou vizuální a funkční kontrolu plynového automatického hasícího systému (SHZ), včetně všech souvisejících komponent. Cílem kontroly je ověření provozuschopnosti systému, jeho souladu s technickými specifikacemi výrobce, projektovou dokumentací a podmínkami prostředí. Kontrola musí být prováděna kvalifikovaným servisním technikem.

1.39.1 Roční kontrola provozuschopnosti systému SHZ

Rozsah provozní kontroly tlakové nádoby:

- Vizuální kontrola stavu systému
- Ověření umístění dle projektové dokumentace

- Kontrola výrobního čísla
- Kontrola uchycení systému, případná oprava
- Ověření přístupnosti systému, případná úprava
- Očištění systému od nečistot

Rozsah provozní kontroly manometru:

- Optická kontrola tlaku
- Kontrola aretace manometru
- V případě nízkého tlaku – dotlakování pomocí certifikovaného zařízení
- Kontrola plomby, případná výměna

Rozsah provozní kontroly tlakového spínače:

- Ověření přenosu signálu na rozhraní řídící jednotky
- Funkční test pomocí kalibrovaného měřidla
- Kontrola plomby, případná výměna

Rozsah provozní kontroly záložního zdroje SHZ:

- Test funkce záložního akumulátoru – provoz na zálohu po dobu 1 hodiny,
- Kontrola spojů napájecího zdroje
- Měření napětí na konci napájecí větve
- Měření izolačního odporu dle elektrorevize

Rozsah provozní kontroly nadřízeného systému EPS:

- Test aktivace hašení z centrály EPS
- Kontrola výstupních signálů (tlak, porucha)
- Test přenosu stavů na vyšší dozorová centra

Rozsah provozní kontroly detekce a ručního startu hašení:

- Test poruchy hlásicí linky vyjmutím hlásiče
- Test funkce hlásičů pomocí testovací sady
- Kontrola ručního hlásiče testovacím klíčem
- Měření impedance hlásicích linek

Rozsah provozní kontroly hlásičů tlaku v zásobnících hasiva:

- Vizuální kontrola tlakových spínačů
- Simulace stavu ztráty tlaku
- Měření impedance hlásicí linky

Rozsah provozní kontroly výstupních zařízení:

- Vizuální kontrola signalizačních prvků
- Funkční test optické a akustické signalizace
- Simulace stavu hašení
- Měření přídržné síly cívky magnetů
- Měření impedance ovládací linky
- Nasazení cívek magnetů

Rozsah provozního testu ústředny:

- Připojení k PC, test obslužným SW po dobu 1 hodiny, vyhodnocení výsledků

Rozsah provozní kontroly kontrolního štítku:

- Kontrola umístění a stavu štítku
- Nalepení štítku dle vyhlášky č. 246/2001 Sb., §7 odst. 4

Garanční zápis:

- Zápis do provozního deníku
- Vyhotovení protokolu o kontrole provozuschopnosti

1.39.2 Půlroční kontrola provozuschopnosti systému SHZ

Rozsah provozní kontroly záložního zdroje:

- Test funkce záložního akumulátoru – provoz na zálohu po dobu 1 hodiny,
- Kontrola spojů napájecího zdroje
- Měření napětí na konci napájecí větve
- Měření izolačního odporu dle elektrorevize

Rozsah provozní kontroly nadřízeného systému EPS:

- Test aktivace hašení z centrály EPS
- Kontrola výstupních signálů (tlak, porucha)
- Test přenosu stavů na vyšší dozorová centra

Rozsah provozní kontroly detekce a ručního startu hašení:

- Test poruchy hlásicí linky vyjmutím hlásiče
- Test funkce hlásičů pomocí testovací sady
- Kontrola ručního hlásiče testovacím klíčem
- Měření impedance hlásicích linek

Rozsah provozní kontroly hlásičů tlaku v zásobnících hasiva:

- Vizuální kontrola tlakových spínačů
- Simulace stavu ztráty tlaku
- Měření impedance hlásicí linky

Rozsah provozní kontroly výstupních zařízení:

- Vizuální kontrola signalizačních prvků
- Funkční test optické a akustické signalizace
- Simulace stavu hašení
- Měření přídržné síly cívky magnetů
- Měření impedance ovládací linky
- Nasazení cívek magnetů

Rozsah provozního testu ústředny:

- Připojení k PC, test obslužným SW po dobu 1 hodiny, vyhodnocení výsledků

Garanční zápis:

- Zápis o provedené kontrole provozuschopnosti zařízení do provozního deníku

1.40 Profylaktické kontroly a revize bleskosvodné a uzemňovací soustavy

Dodavatel je povinen zajistit pravidelnou vizuální a funkční kontrolu bleskosvodné a uzemňovací soustavy (LPS), včetně všech souvisejících komponent. Cílem kontroly je ověření provozuschopnosti systému, jeho souladu s technickými specifikacemi výrobce, projektovou dokumentací a podmínkami prostředí. Kontrola musí být prováděna kvalifikovaným servisním technikem.

Dodavatel je povinen zajistit pravidelné revize bleskosvodné a uzemňovací soustavy (LPS) definované pro objekty kritické infrastruktury v ČR, podle normy **ČSN EN 62305-3 ed.2** a souvisejících předpisů. Kontrola musí být prováděna kvalifikovaným revizním technikem, a to v minimálně v rozsahu:

- **Výchozí revize** – před uvedením do provozu nebo po rekonstrukci
- **Pravidelná revize** – každé **2 roky** (kritická infrastruktura)
- **Mimořádná revize** – po zásahu bleskem, přesunu, opravách

Rozsah provozní kontroly bleskosvodné a uzemňovací soustavy (1x ročně):

- Kontrola jímací soustavy (tyče, lana, mříže)
- Kontrola svodů – neporušenost, uchycení, vedení
- Kontrola uzemňovací soustavy – přístupnost, značení
- Kontrola spojů – mechanické poškození, koroze
- Kontrola ekvipotenciálního pospojování
- Zkouška a měření rozpojení zkušebních svorek
- Měření zemního odporu
- Kontrola přepěťových ochran – funkčnost, stav
- Vyhotovení protokolu o kontrole provozuschopnosti

1.41 Profylaktické kontroly a revize nouzového osvětlení

Dodavatel je povinen zajistit pravidelnou vizuální a funkční kontrolu a údržbu nouzového osvětlení**,** včetně všech souvisejících komponent dle normy **ČSN EN 50172**. Cílem kontroly je ověření provozuschopnosti systému, jeho souladu s technickými specifikacemi výrobce, projektovou dokumentací a podmínkami prostředí.

Kontrola musí být prováděna kvalifikovaným servisním technikem nebo **automatickým testovacím systémem**, s výstupem do trvalého záznamového média (provozní deník)

Rozsah provozní kontroly nouzového osvětlení (1x měsíčně):

- Funkční test každého svítidla – simulace výpadku napájení
- Ověření, že svítidla se rozsvítí a fungují po stanovenou dobu
- Záznam výsledků do provozního deníku

Rozsah provozní kontroly nouzového osvětlení (1x ročně):

- Dlouhodobý test – simulace výpadku napájení na celou dobu autonomie (např. 1 hodina)
- Kontrola kapacity baterií, funkčnosti centrálního napájení
- Záznam do provozního deníku + vystavení dokladu o provedení zkoušky

Dokumentace a podpůrný software

1.42 Dokumentace skutečného provedení

Zadavatel požaduje, aby Dodavatel po dokončení instalace a uvedení mobilního kontejnerového datového centra do provozu předal kompletní **dokumentaci skutečného provedení díla**. Tato dokumentace musí obsahovat zejména:

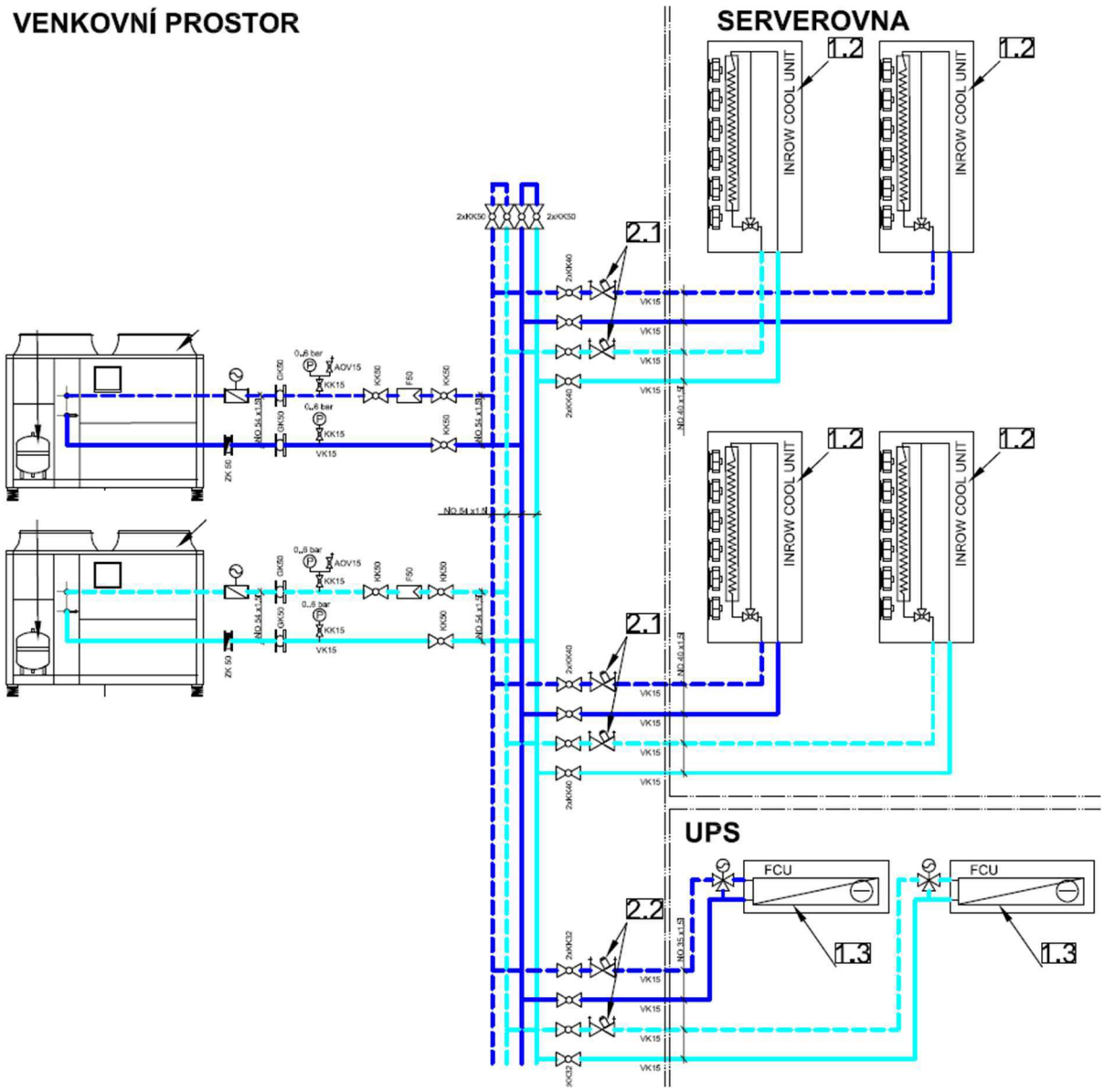
- Aktuální výkresovou dokumentaci skutečného stavu (včetně elektroinstalace, chlazení, napájecích větví, ICT infrastruktury apod.)
- Schémata zapojení a technické listy použitých zařízení
- Seznamy instalovaných komponent včetně výrobních čísel
- Revizní zprávy a protokoly o funkčních zkouškách
- Provozní a údržbové manuály
- Záznamy o konfiguraci systémů (např. UPS, monitoring, SHZ)
- A další relevantní dokumenty dle charakteru dodávky

Dokumentace musí být předána v **elektronické podobě** (ve formátu PDF a editovatelném formátu, např. DWG, DOCX, XLSX), a to nejpozději při předání a převzetí díla.

Ideologické schémata serverovny SŽT

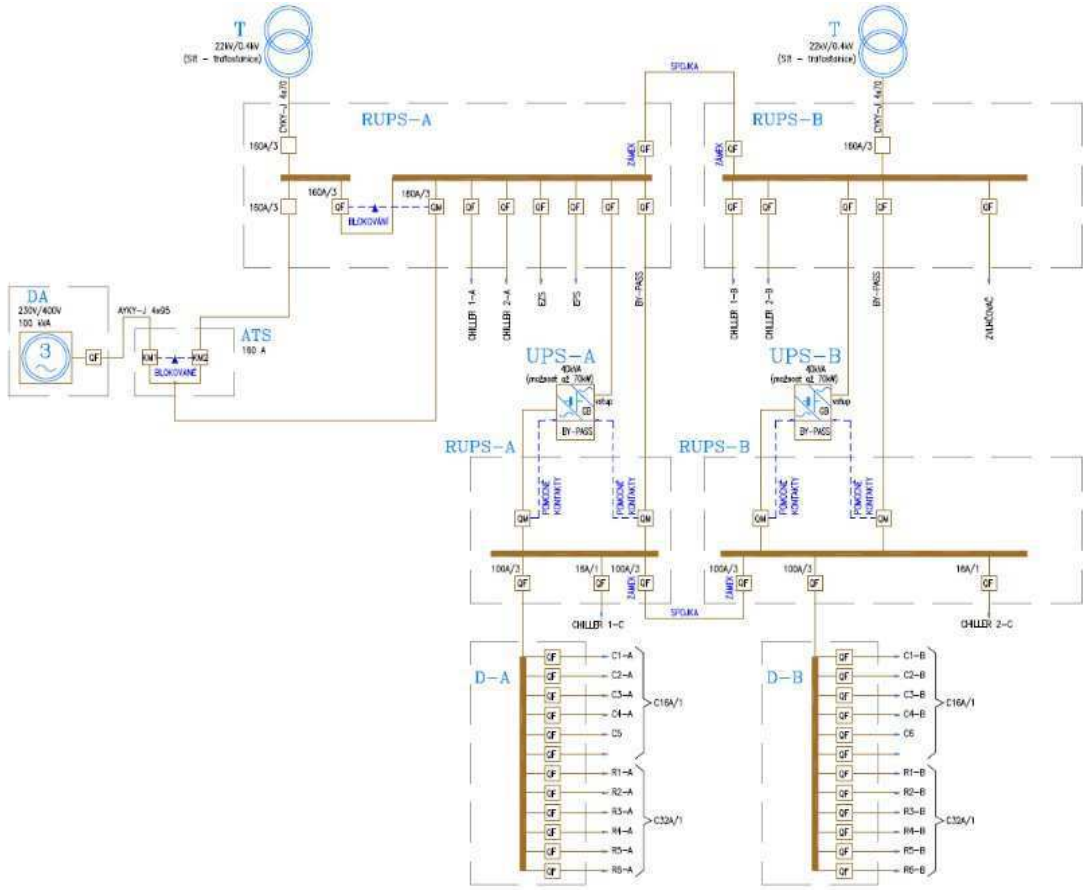
1.43 Ideologické schéma zapojení chlazení serverovny

Schéma níže je koncepčním návrhem zapojení chlazení serverovny, má sloužit jako podklad pro další technický návrh a neslouží jako závazný technický návrh.



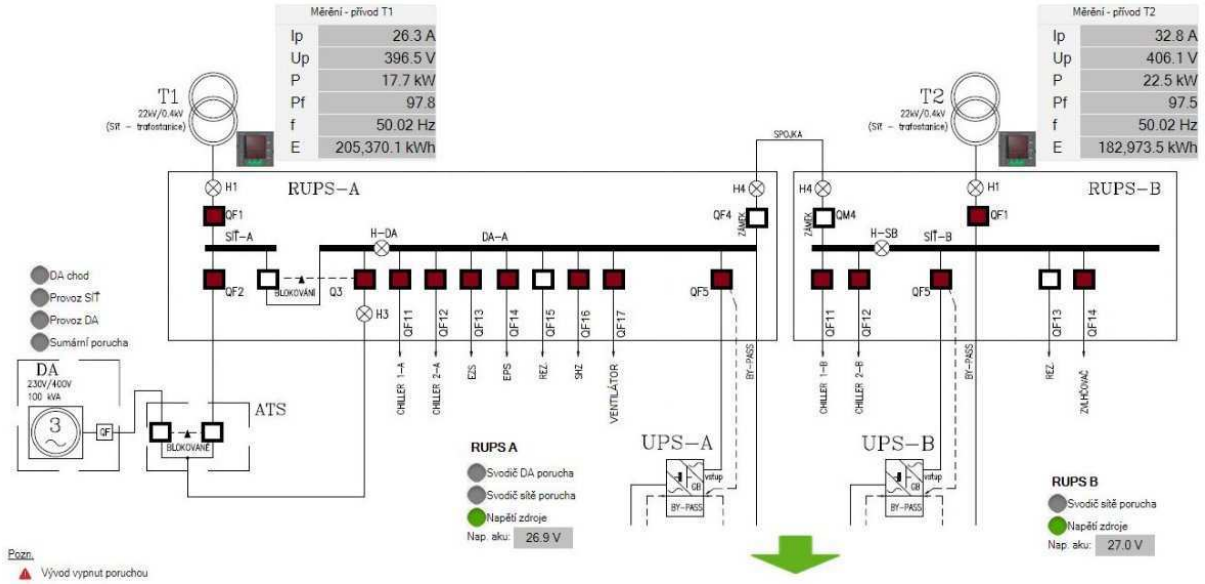
1.44 Ideologické schéma zapojení napájení serverovny

Schéma níže je koncepčním návrhem zapojení napájení serverovny, má sloužit jako podklad pro další technický návrh a neslouží jako závazný technický návrh.



1.45 Ideologické schéma vizualizace monitorovaného prostředí serverovny

Schéma níže je koncepčním návrhem vizualizace monitorovaného prostředí datového centra, má sloužit jako podklad pro další technický návrh a neslouží jako závazný technický návrh.



Seznam použitých zkratek

V tomto dokumentu a jeho přílohách jsou použity nebo se mohou vyskytovat především následující zkratky:

ZKRATKA	VÝZNAM	PŘEKLAD / POPIS
CAPEX	Capital Expenditure	investiční náklady
EIA	Electronic Industries Alliance	aliance výrobců elektroniky v USA, vydává normy
OPEX	Operating Expense	provozní náklady
TCO	Total Cost of Ownership	celkové náklady (na) vlastnictví
TIER	není zkratka	klasifikace datových center z hlediska dostupnosti, lze certifikovat DC nebo i projekt
HC	High Cube	Velikost kontejneru dle ISO
FAT	Factory Acceptance Test	Testování při zatížení ve výrobním závodě
TCCF	Tier Certification of Costructed Facility	Certifikace souladu TIER realizovaného datového centra
TCDD	Tier Certification Design Documents	Certifikace souladu TIER projektové dokumentace datového centra
PUE	Power Usage Effectiveness	koeficient definující energetickou účinnost datového centra; celkový příkon DC/příkon IT
AC	Alternating Current	střídavý proud
ATS	Automatic Transfer Switch	rozvaděč sloužící pro přepínání provozu ze sítě na náhradní zdroj
CU	Control Unit	řídící jednotka v obecném slova smyslu
DC	Dirrect Current	stejnosměrný proud
MaR	Měření a Regulace	měření a regulace
MG/DA	Motorgenerátor	motorgenerátor
nn	nízké napětí	nízké napětí
PDU	Power Distribution Unit	napájecí lišta zpravidla umístěná v serverové skříni (nejčastěji

		osazena větším množstvím zásuvek dle IEC60320, typ C13 resp. C19)
PHM	pohonné hmoty	pohonné hmoty
RCH	Rozvaděč Chlazení	rozvaděč, z kterého jsou napájeny části chladicího systému (zdroje chladu, klimatizační jednotky, čerpadla apod.)
RTN	Rozvaděč Trvalého Napájení	rozvaděč, který je napájen ze zálohovaného napájení ze zdroje UPS
RUPS	Rozvaděč UPS	rozvaděč sloužící pro připojení vstupu a výstupu zdroje UPS a zpravidla umožňuje i bypass tohoto zdroje
ŘS	Řídicí Systém	řídicí systém
TN-C	Terre - Neutre - Combine	rozvodná síť s uzemněným uzlem, s použitím ochranného vodiče, který je společný se středním vodičem
TN-S	Terre - Neutre - Separé	rozvodná síť s uzemněným uzlem, s použitím ochranného vodiče a samostatným středním vodičem
UPS	Uninterruptible Power Supply	zdroj záložního napájení
LVD	Low Voltage Disconector	Odpojovač při nízkém napětí baterií
Ethernet		nejrozšířenější technologie pro budování počítačových sítí typu LAN
GSM	Global System for Mobile Communications	mezinárodní standard plně digitálních mobilních sítí
ICT, IT	Information (Communication) Technology	informační technologie
LAN	Local Area Network	označuje počítačovou síť, která pokrývá malé geografické území
PoE	Power over Ethernet	napájení po datovém síťovém kabelu, bez nutnosti přivést

		napájecí napětí k přístroji dalším samostatným kabelem
SAN	Storage Area Network	datová síť, která slouží pro připojení externích zařízení k serverům (disková pole, páskové knihovny a jiná zálohovací zařízení).
SLA	Service Level Agreement	definice rozsahu, úrovně a intenzity služeb poskytovaných dodavatelem zákazníkovi
SNMP	Simple Network Management Protocol	protokol určený pro správu zařízení
TCP/IP	Transmission Control Protocol / Internet Protocol	sada protokolů pro komunikaci v počítačové síti
VPN	Virtual Private Network	virtuální privátní síť, princip, který umožní připojení do sítě tak, aby nemohla být narušena integrita a důvěrnost přenášených dat
WAN	Wide Area Network	počítačová síť, která pokrývá rozlehlé geografické území
Wifi	Wireless fidelity	standard pro bezdrátovou lokální počítačovou síť
WWW	World Wide Web	označení pro aplikace internetového protokolu HTTP
AHU	Air Handling Unit	jednotka zajišťující úpravu a cirkulaci vzduchu (vzduchotechnická jednotka)
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers	asociace inženýrů v oblasti vytápění, chlazení a klimatizace, jejímž cílem je rozvoj HVAC
DX	Direct Expansion	chlazení metodou přímé expanze, výparník je v přímém kontaktu s proudem chlazeného vzduchu
FC	Free Cooling	volné chlazení (využívá se příznivě nízké venkovní teploty)
HVAC	Heating, Ventilation and Air Conditioning	vytápění, vzduchotechnika a klimatizace
HX	Heat Exchange	Výměna tepla

MMDC	Modular Mobile Data Centre	modulární mobilní datové centrum (zpravidla kontejnerové provedení)
ACS/EKV/SKV	Access Control System /Elektronická Kontrola Vstupu/Systém kontroly Vstupu	elektronický přístupový systém
CCTV	Closed Circuit TV	uzavřený televizní okruh, kamerový systém
EPS	Elektronická Požární Signalizace	elektronická požární signalizace
EZS	Elektronický Zabezpečovací Systém	elektronický zabezpečovací systém
PZTS	Poplachový Zabezpečovací a Tísňový Systém	elektronický zabezpečovací systém
SHZ	Stabilní Hasicí Zařízení	automatický stabilní hasicí systém
EMC	Electromagnetic Compability	elektromagnetická kompatibilita
EMI	Electromagnetic Interference	elektromagnetické rušení

----------KONEC----------

SPRÁVA ŽELEZNIC

Realizace systému zabezpečeného úložiště v prostředí Správy železnic

(Příloha č. 3 Pozvánky - Technická specifikace předmětu plnění)

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

Klasifikace: Veřejný dokument

Obsah

1 Seznam pojmů a zkratek

Níže uvedená tabulka obsahuje seznam zkratek a pojmů použitých v rámci této Technické specifikace.

Přehled zkratek a pojmů:

Zkratka	**Popis**
Dodavatel	Účastník zadávacího řízení, který bude ze strany SŽ vybrán k uzavření smlouvy
HTTP(S), DNS, SNMP, SMTP, FTP, TFTP	Komunikační protokoly
HW	Hardware
IdM	Systém správy identit popisuje řízení jednotlivých identit, jejich autentizaci, autorizaci, role a privilegia v rámci nebo přes hranice systému a organizace s cílem zvýšit bezpečnost a produktivitu při současném snížení nákladů, prostojů a opakujících se úkolů *(Identity Management)*
ICT	Informační a komunikační technologie (Information and Communication Technologies)
IS	Informační systém
KII	Kritická informační infrastruktura
RADIUS, TACACS+, SAML, IPSec	Autentizační protokoly
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OS	Operační systém *(Operating System)*
PTK	Předběžná tržní konzultace je nástroj umožňující zadavateli veřejné zakázky oslovit dodavatele s požadavkem na informace ohledně zamýšlené připravované veřejné zakázky *(Request for Information)*
RBAC	Řízení přístupů na základě rolí
SIEM	Řešení zabezpečení, které organizacím pomáhá detekovat bezpečnostní události, analyzovat je a reagovat na ně dříve, než

	způsobí škody v provozu firmy/organizace. *(Security Information and Event Management)*
SLA	Smluvní nastavení záruk, úrovně, dostupnosti a kvality služeb atd. *(ServiceLevel Agreement)*
SW	Programové vybavení počítače či jiného obdobného zařízení. Speciálním druhem software je *firmware*, který je úzce spjatý s konkrétním hardwarem *(Software)*
SŽ	Správa železnic, státní organizace („Zadavatel“)
Účastník	Subjekt, který se účastní tohoto zadávacího řízení o realizaci veřejné zakázky
VZ	Veřejná zakázka
VoKB	Vyhláška č. 409/2025 Sb. o bezpečnostních opatřeních, poskytovatele regulované služby v režimu vyšších povinností, ve znění pozdějších předpisů
ZD	Zadávací dokumentace
ZoKB	Zákon č. 264/2025 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

2 Úvod

Tento dokument slouží jako veřejný podklad pro předběžnou tržní konzultaci (PTK) k plánovanému zadávacímu řízení na veřejnou zakázku „Realizace systému zabezpečeného úložiště v prostředí Správy železnic". Cílem je popsat požadavky na hardware, software a související oblasti tak, aby budoucí zadávací dokumentace mohla být formulována přesně, technologicky neutrálně a nediskriminačně, s ohledem na potřeby Zadavatele a legislativní rámec.

Zadavatel plánuje vybudovat centralizované bezpečné datové úložiště v rámci Programu kybernetické bezpečnosti pro Správu železnic. Toto bezpečné úložiště má zajistit správu, ukládání a archivaci důležitých dat napříč vybranými informačními systémy a technologiemi. Projekt bude spolufinancován z programu IROP (Integrovaný regionální operační program), a musí tedy naplnit definovaná bezpečnostní opatření a indikátory tohoto programu.

2.1 Hlavní cíle

Bezpečné datové úložiště bude navrženo tak, aby splnilo následující klíčové cíle:

- **On-premises**: Celé řešení bezpečného úložiště musí být provozováno v on-premises prostředí Správy železnic, tedy výhradně v rámci její vlastní infrastruktury. Žádná data nesmí opustit perimetr interní sítě, a to včetně ukládání nebo přenosu do veřejného cloudu či jiných externích služeb.
- **Vysoká dostupnost dat:** Data musí být dostupná i při výpadku lokality díky geograficky odděleným clusterům a replikaci mezi lokalitami (geo-clustering). Toto minimalizuje riziko ztráty dat při havárii jednoho datového centra.
- **Bezpečné řízení přístupu:** Centralizovaná správa přístupů a autentizace k uloženým datům – přístupy budou jednotně řízeny a auditovány, aby byla zajištěna důsledná kontrola nad tím, kdo může s daty nakládat.
- **Ochrana a šifrování dat:** Zabezpečené ukládání dat s využitím silného šifrování a bezpečné správy klíčů. Nasazen bude Hardware Security Module (HSM) pro ukládání a správu kryptografických klíčů, aby uložená data nebylo možné číst bez autorizace.
- **Odolnost vůči incidentům:** Infrastruktura úložiště bude navržena pro vysokou odolnost (disaster recovery). Bude zahrnovat záložní napájení, monitorování prostředí a další prvky fyzické i logické ochrany, aby byl zajištěn nepřetržitý provoz i při mimořádných událostech.
- **Soulad s legislativou a standardy:** Řešení zohlední legislativní požadavky na ochranu KII, kybernetickou bezpečnost a ochranu osobních údajů. Bude splňovat požadavky NÚKIB (národní úřad pro Kybernetickou bezpečnost) dané zákonem a vyhláškou v platném znění, včetně implementace opatření jako správa identit, řízení přístupových oprávnění, kryptografické prostředky, fyzická bezpečnost a zajištění dostupnosti informací. Dále bude brán zřetel na doporučení mezinárodních standardů (např. ISO/IEC 27001, NIST CSF) a osvědčené postupy.

3 Požadované komponenty a infrastruktura řešení

SŽ předpokládá, že řešení bezpečného úložiště bude zahrnovat následující.

3.1 Prostor datového centra pro Bezpečné datové úložiště

Datové centrum: Prostor pro bezpečné datové úložiště bude formou mobilního kontejnerového datového centra pro centrální a záložní lokalitu umístěné v areálu SŽ

- **Specifikace požadavků na datový kontejner:**
- Řešení je specifikováno v samostatném dokumentu: Příloha 2_Pozvánky - *Technická specifikace předmětu plnění - Mobilní kontejnerové datové centrum*

3.2 Disková úložiště a kapacita pro data

- **Disková pole:** Navržené řešení musí zajistit dostatečnou kapacitu a výkon pro data vybraných systémů. Plánuje se pořízení nových diskových úložišť (diskových polí) pro tyto klíčové systémy. Disková pole budou umístěna v centrální a záložní lokalitě a kapacitně pokryjí současné potřeby, včetně rezervy pro budoucí růst dat. Součástí dodávky musí být i potřebný software pro centrální správu úložišť. Výchozí kapacita čisté nekomprimované kapacity je zvažována minimálně **6 PB (petabajtů)** pro každou lokalitu.
- **Geografická redundance dat:** Počítá se s nasazením diskových polí také v záložní lokalitě (druhé datové centrum) pro účely geo-redundance. Data budou replikována z primárního úložiště do sekundárního (viz kapitola o dostupnosti níže), tudíž i záložní lokalita musí disponovat dostatečnou kapacitou disků. Primární i sekundární disková pole by měla být technicky podobná/kompatibilní, aby umožnila efektivní replikaci a případný rychlý převod provozu. Pole musí umožnovat provoz v režimu Active-Passive a Active-Active.
- **Výkon a technologie disků:** Vzhledem k očekávanému charakteru dat (kombinace často využívaných provozních dat a archivních záloh) je požadováno víceúrovňové úložiště – Hybrid Storage.
  - Kritická, často přístupná data KII budou uložena na vysokorychlostních discích (typu NVMe/SAS SSD) s možnou podporou Hot Swap. Tyto disky musí umožnovat velký počet cyklů přepisu dat.
  - Objemná archivní nebo méně využívaná data budou uložena na rotačních discích s vysokou kapacitou (typu SAS, NL-SAS) s podporou Hot Swap. Tyto

disky musí umožnovat dlouhodobou čitelnost dat. Tento storage tiering zajistí optimální poměr výkonu a nákladů. Řešení by mělo podporovat automatizované přesouvání dat mezi tiery dle nastavených politik (např. po určité době neaktivity přesun na pomalejší úložiště).

- **Rozšiřitelnost kapacity:** Úložiště musí být škálovatelné pro budoucí růst – architektura by měla umožňovat přidání dalších diskových shelfů či uzlů bez výpadku provozu. V současné fázi není přesná velikost dat KII známa (bude upřesněno v průběhu projektu), avšak očekává se nárůst. Dodavatelé by měli nabídnout řešení, které lze kapacitně navýšit (řádově v desítkách % ročně) a případně využívá i techniky deduplikace a komprese, aby se efektivní kapacita maximalizovala.
- **Výkonové požadavky:** Krom kapacity je důležitá i propustnost a IOPS. Systém musí zvládat simultánní zápis záložních dat z více zdrojů a případně i čtení při obnově, bez úzkých hrdel. Zálohovací systém a servery
- **Testování obnovy:** Řešení by mělo umožnit provádět zkoušky obnovy (např. do izolovaného prostředí) tak, aby SŽ měla jistotu, že zálohy jsou validní a použitelné. V rámci provozních procesů bude zaveden plán periodických testů: například čtvrtletně provést obnovu vybraného kritického systému ze zálohy a vyhodnotit, zda odpovídá požadovanému RTO/RPO.
- **Síťová infrastruktura:** Součástí dodávky musí být i redundantní síťová infrastruktura LAN případně i SAN (pokud je třeba) o dostatečné kapacitě, aby nevznikala úzká hrdla v rámci zápisu, čtení a redistribuce a replikace dat. Řešení bude provozováno s využitím 100Gb/s datového propojení. Součástí dodávky musí být zabezpečení komunikace v rámci prostředí bezpečného úložiště, včetně ochrany vnějšího perimetru ve formě firewallů. Tato ochrana musí splňovat vysokou dostupnost a dále musí mít schopnost inspekce datového toku a kontroly obsahu procházejících dat vůči definovaným signaturám (DLP systém).

3.3 Zálohovací systém a servery

- **Konsolidace zálohování:** Jedním z cílů aktivity je centralizovat a posílit zálohovací kapacity SŽ. Za tímto účelem budou pořízeny i zálohovací servery (backup servery) – tj. výkonné serverové jednotky s potřebným software, které budou spravovat proces zálohování a uchovávat záložní kopie na diskových polích úložiště. Tyto servery se stanou integrální součástí Bezpečného úložiště. Ochrana záloh proti útokům: Úložiště musí mít implementována opatření, jež zabrání kompromitaci záloh, využitím neměnných úložišť pro zálohy nebo jiných mechanismů, které znemožní dodatečnou úpravu či mazání záloh po jejich vytvoření po definovanou dobu. Například zálohovací software může podporovat funkci immutable backup (nastavení nezměnitelnosti souborů) či WORM úložiště (Write Once Read Many).
- **Testování obnovy:** Kromě samotného ukládání záloh by řešení mělo umožnit provádět zkoušky obnovy (např. do izolovaného prostředí) tak, aby SŽ měla jistotu, že zálohy jsou validní a použitelné. V rámci provozních procesů bude

zaveden plán periodických testů: například čtvrtletně provést obnovu vybraného kritického systému ze zálohy a vyhodnotit, zda odpovídá požadovanému RTO/RPO.

4 Požadavky na funkčnost a vlastnosti řešení

4.1 Vysoká dostupnost a geografická redundance

Pro maximální odolnost proti výpadkům, musí být úložiště navrženo s architekturou pro vysokou dostupnost s geografickou redundancí. Konkrétně požadujeme:

- **Geo-cluster (min. dvě lokality):** Data budou uložena a replikována mezi alespoň 2 fyzicky oddělenými lokalitami – primární (hlavní DC) a sekundární DC. Replikace může být synchronní (pro nejnáročnější data s nulovou ztrátou, pokud to latence dovolí) nebo asynchronní, vždy ale s dohledem na integritu dat. Při výpadku primárního místa bude možné provoz obnovit ze záložního s minimalizovaným výpadkem. Parametry RTO a RPO pro jednotlivé typy dat budou stanoveny podle kritičnosti (např. nejkritičtější data KII RTO v řádu hodin, méně důležitá mohou mít desítky hodin).
- **Clusterová architektura a failover:** Samotné úložiště v primární lokalitě by mělo být navrženo jako cluster (více uzlů nebo dual-controller systém), aby i lokální porucha zařízení neznamenala nedostupnost služby. Při poruše některého z prvků (server, kontroler diskového pole, síťový prvek) musí zátěž automaticky převzít redundantní prvek. V případě úplného výpadku celé primární lokality bude spuštěn disaster recovery plán, kdy sekundární lokalita převezme poskytování služby úložiště. Tento failover proces musí být definován a otestován – ideálně automatizovaně či poloautomatizovaně, aby zásah obsluhy byl minimální a obnova rychlá.
- **Dostupnost služby:** Systém by měl cílit na vysokou dostupnost ve smyslu průměrné doby provozu. Reálně očekáváme dosažení dostupnosti nejméně 99,9 % (odpovídá max. ~8,8 hod výpadku ročně) pro kritické části, spíše však vyšší.
- **Retence a obnova dat:** Kromě dostupnosti služeb je důležité i zachování dat a jejich obnova. Úložiště proto bude podporovat definované retenční doby pro různá data (např. uchování záloh X měsíců/let dle typu systému) a archivaci. Při návrhu DR plánu se stanoví, které zálohy se uchovávají i mimo online přístup (např. dlouhodobé zálohy offline na páskách uložených mimo lokalitu pro zajištění ultimátní zálohy). Procesy budou nastaveny tak, aby v případě nouze byla dostupná alespoň jedna nezasažená kopie dat.

4.2 Škálovatelnost a tiering úložiště

- **Modulární rozšíření:** Řešení musí být schopné růst s požadavky na kapacitu i výkon. Objem ukládaných dat (např. z nových systémů KII nebo delších retenčních dob) se bude v čase zvyšovat. Proto upřednostňujeme modulární systém, který

umožňuje přidávat diskové moduly, uzly nebo výkonové komponenty postupně podle potřeby.

- **Storage tiering a životní cyklus dat:** Jak již bylo zmíněno, data budou uložena podle frekvence použití a důležitosti do odpovídajících úložných vrstev (tiers). Systém musí umožňovat automatizovanou správu životního cyklu dat – tzn. definovat politiky, kdy se data přesouvají mezi vrstvami. Např. primární ostrá data kritických aplikací budou na nejrychlejším úložišti; po určité době nebo při změně statusu (archivace) se mohou přesunout na levnější, pomalejší úložiště. Správné nastavení tieringu zajistí, že často využívaná data mají vysoký výkon, zatímco pro archivní účely je k dispozici velká kapacita. To vše transparentně pro uživatele a aplikace. Použitý systém by měl umět využít metadata (datum posledního přístupu, označení archivu apod.) k automatickému tieringu.
- **Výkonové škálování:** Kromě kapacity je podstatná i škálovatelnost výkonu – například přidat další front-end kontrolery k diskovým polím, navýšit síťovou propustnost replikace mezi lokalitami nebo posílit počet zálohovacích serverů při zapojení dalších systémů do zálohování. Systém by neměl trpět bottlenecky, které by se zhoršovaly s rostoucí zátěží.

4.3 Zabezpečení dat a šifrování

Bezpečnost uložených dat je absolutní prioritou, jelikož může jít i o data kritické informační infrastruktury. Požadujeme tedy vícevrstvou ochranu:

- **Šifrování dat v klidu (at rest):** Veškerá data uložená v Bezpečném úložišti musí být šifrována moderními silnými algoritmy. Ideálně bude šifrování probíhat na úrovni diskových úložišť nebo file systémů automaticky, transparentně pro aplikace. Tím se zajistí, že i v případě fyzického získání disků nebo neautorizovaného přístupu k úložišti útočník data nevyužije bez klíčů. Implementace musí být v souladu s politikami SŽ a požadavky legislativy (zákon o Kybernetické bezpečnosti, nebo GDPR pro osobní údaje). Disková pole musí mít možnost integrace s externím HSM (Hardware Security Module), pro management šifrovacích klíčů.
- **Šifrování dat v přenosu (in transit):** Data přenášená z/do úložiště musí být chráněna. Všechny komunikace mezi zálohovanými servery, klienty a úložištěm proběhnou výhradně přes šifrované kanály (např. SSH, TLS 1.3, IPsec, L2TP).
- **Správa šifrovacích klíčů (KMS/HSM):** Řešení bude podporovat Hardware Security Module (HSM) pro generování, bezpečné ukládání a správu kryptografických klíčů. SŽ již HSM v nějaké formě využívá – úložiště musí umožnit integraci s HSM (typicky prostřednictvím protokolu PKCS#11 nebo KMIP). Všechny klíče k šifrování dat úložiště budou spravovány tímto centrálním HSM modulem, případně úložiště bude mít vlastní HSM.
- **Ochrana proti škodlivému kódu:** Data budou chráněna proti škodlivým kódům (Malware, ransomware…). Na vstupu do úložiště (při zápisu dat ze systémů) mohou být nasazeny bezpečnostní nástroje na detekci známého malware

(antivirové skeny záloh atd.). Cílem je, aby uložené zálohy již neobsahovaly například „spící ransomware. Tato kontrola spadá pod opatření "ochrana před škodlivým kódem" dle vyhlášky – a bude realizována integrací se stávajícím skenovacím XDR nástrojem.

- **Integrita a detekce změn:** Systém by měl umět ověřovat integritu uložených dat (například skrze kontrolní součty, které detekují tichou korupci dat, tzv. bit rot, nebo neautorizovanou změnu). Řízení přístupu a správa identit

Pro efektivní a bezpečný přístup k datům musí systém umožňovat řízení přístupových oprávnění:

- **Centralizovaná autentizace a autorizace**: Nové úložiště se plně začlení do stávajícího systému pro správu identit Identity Management (IdM) a a do stávajícího systému pro vzdálený přístup Privileged Access Management (PAM). Uživatelé (nebo služby) přistupující k datům úložiště budou ověřováni proti centrální databázi účtů (např. Active Directory/ADFS). Přístupová práva k datům pak budou udělována na základě rolí definovaných v IdM a/nebo skupin v AD – například administrátoři záloh, auditní role, běžní uživatelé konkrétní aplikace apod. Tím se zajistí jednotné přihlašování (Single Sign-On) a především efektivní a přehledná správa přístupových oprávnění.
- **Role-Based Access Control:** Systém musí podporovat RBAC – přiřazování oprávnění podle role. Např. administrátor úložiště může spravovat infrastrukturu, ale nedostane se k obsahu záloh konkrétní aplikace, pokud k tomu není důvod. Naopak správce dané aplikace může mít právo obnovit její data ze zálohy, ale nevidí jiné části úložiště. Tato granulární oprávnění lze spravovat přes IdM/PAM nebo lokálně v úložišti, ale preferujeme centralizaci. Privilegované účty (správci systému) by měly být spravovány právě přes PAM s minimem trvalých přístupů a případně vyžadovat víceúrovňové schválení pro nejcitlivější operace.
- **Důsledná autentizace:** Pro administrativní přístupy vyžadujeme vícefaktorovou autentizaci (MFA). Ať už přes integraci s existující MFA SŽ, nebo vlastnostmi IdM/PAM.
- **Audit a záznamy přístupů:** Systém musí logovat veškeré přístupy k datům i administrativní akce minimálně v rozsahu požadovaném Vyhláškou č. 409/2025 Sb. Každé přečtení či obnova záložního souboru, každá změna nastavení, přidání uživatele apod. Tyto logy budou dlouhodobě uchovávány pro potřeby auditu a v souladu s legislativou (např. zákon o KB vyžaduje určitou dobu uchování záznamů o událostech). Mimo interního logování budou údaje předávány i do centrálního log managementu a SIEM (viz dále). Systém musí podporovat běžné formáty log souborů (např. CLF, ELF, SysLog, JSON...).
- **Oddělení prostředí a tenantů:** Úložiště může sloužit více různým agendám (více systémům). Je žádoucí, aby bylo možné logicky oddělit data jednotlivých skupin systémů či útvarů (tzv. multitenancy). Například data provozních technologických systémů mohou být ve vyhrazeném oddílu, logicky odděleném od dat ekonomických systémů, pokud to správu zjednoduší a zvýší přehlednost přístupů.

Oddělení by však nemělo bránit centrální správě – je to logická vrstva navíc pro případnou granularitu oprávnění.

4.4 Integrace, monitorování a dohled

Pro efektivní provoz úložiště, systém musí zapadat do ekosystému stávajících nástrojů pro správu a bezpečnostní dohled SŽ:

- **Kompatibilita s IT prostředím SŽ:** Navržené úložiště bude plně kompatibilní s existujícími systémy a technologiemi, které jej budou využívat. To zahrnuje podporu běžných standardních protokolů pro přístup k datům – např. CIFS/SMB, NFS pro souborové sdílení, příp. blokové protokoly (iSCSI, Fibre Channel) pro připojení databázových serverů. Úložiště by mělo umožnit snadnou integraci do virtualizační platformy (VMware vSphere) a do clusterových prostředí, pokud některé systémy používají sdílená datová úložiště.
- **Napojení na monitorovací systémy:** Infrastruktura bude připojena k centrálnímu monitoringu SŽ tak, aby stav hardware (disky, zdroje, teploty), služby replikací a záloh byly neustále sledovány operátory. Výpadky, pokles výkonu nebo poruchy komponent budou automaticky hlášeny. Dále bude systém poskytovat telemetrii výkonu – využití kapacity, IO, síťové přenosy – pro účely kapacitního plánování. Budou podporovány běžné protokoly pro monitoring – SNMPv3, ICMP, HTTPS, IPMI, Storage Insights…
- **SIEM a log management:** Všechny relevantní logy budou odesílány do centrálního Security Information and Event Management (SIEM) systému. Úložiště musí umět exportovat logy standardním způsobem (syslog, případně API integrace) a obsahovat dostatečné informace (uživatelská ID, IP adresy, kódy událostí). Odesílané logy musí být ve standardizovaném formátu JSON, CEF, LEEF atd.
- **Provozní dohled a správa:** Dodané řešení musí zahrnovat nástroj pro správu konfigurace a diagnostiku, např. v podobě centrální management konzole (Unified storage manager) pro veškerá úložiště, s možností skriptování rutinních úloh (Infrastructure as Code).
- **Podpora a SLA:** Součástí bude i plán podpory – včetně například možnosti vzdáleného dohledu typu Call Home, (pokud to bezpečnostní politika dovolí) nebo minimálně jasně definovaných SLA pro podporu. Kritické komponenty by měly mít garantovanou servisní odezvu do X hodin a případně 24/7 podporu, aby případné problémy byly řešeny urgentně. Je požadavek, aby dodavatel v PTK nastínil možnosti podpory (např. lokalizovaný servisní tým v ČR, sklad náhradních dílů atd.). Standardní záruční doba (Limited warranty) na HW minimálně 5 let s možností jejího prodloužení

4.5 Provozní aspekty a testování

- **Provozní dokumentace:** Dodavatel v rámci dodávky poskytne kompletní dokumentaci – administrátorskou příručku, uživatelské návody, popis architektury a konfigurace, bezpečnostní konfigurační údaje, postupy pro běžnou údržbu i obnovu po havárii. Dokumentace bude sloužit jako základ pro rutinní provoz, školení personálu, interní audity a případné kontroly ze strany dozorových orgánů.
- **Školení personálu:** Realizace projektu bude zahrnovat zaškolení administrátorů a dalších pracovníků SŽ, kteří budou úložiště spravovat. Vzhledem k zavedení nových technologií (např. správa kontejnerového DC, práce s HSM, nastavení IdM pro úložiště) je nutné, aby tým získal potřebné dovednosti. Ideálně školení zajistí přímo dodavatel v češtině, případně v angličtině pro vybrané specialisty, a to ještě před uvedením úložiště do produkčního provozu. Následně bude určen provozní tým 24/7, který zajistí nepřetržitý dohled nad úložištěm (může spadat do existujícího týmu kybernetického dohledu SŽ).
- **Testovací provoz a pilot:** Po dodání a instalaci proběhne pilotní provoz – úložiště bude nejprve nasazeno pro omezenou sadu dat/systémů, na kterých se otestuje funkčnost (zejména replikace, zálohování a obnova, výkon). Během pilotu se doladí konfigurace, poté dojde k ostrému zapojení všech plánovaných systémů. Tento postup minimalizuje rizika. V harmonogramu se s pilotním provozem počítá (dle interních plánů Zadavatele) tak, aby ostré spuštění včetně záložního provozu proběhlo **do 10/2026**.

5 Závěr

Navržené Bezpečné úložiště bude představovat centrální bod pro zabezpečenou správu, ukládání a archivaci dat Správy železnic. Kombinací moderní infrastruktury (geo-redundantní datové centrum, výkonná disková pole), přísných bezpečnostních opatření (šifrování, řízení přístupů, fyzická ochrana) a osvědčených postupů (zálohovací strategie 3-2-1, integrace do ekosystému SIEM/IdM) chce Zadavatel dosáhnout požadované vysoké úrovně dostupnosti, bezpečnosti a odolnosti dat KII. Tento dokument by měl sloužit jako výchozí bod pro diskusi s trhem – Zadavatel od potenciálních dodavatelů očekává zpětnou vazbu a informace o možných řešeních, abych v následné zadávací dokumentaci mohl stanovit reálné a optimální požadavky. Cílem je, aby budoucí realizované úložiště splnilo všechny uvedené požadavky a přispělo k celkovému posílení kybernetické bezpečnosti Zadavatele.

Zadavatel prosí účastníky PTK o zodpovězení připravených dotazů (viz Příloha č. 4 - Otázky k zodpovězení PTK) a o doporučení konkrétních postupů či technologií, které by podle jejich zkušeností mohly naplnit výše popsané požadavky. SŽ je otevřena různým variantám řešení, pokud budou v souladu s uvedenými principy. Zadavatel je přesvědčen, že spolupráce s trhem v této fázi mu umožní dosáhnout optimálního výsledku, jímž bude úložiště zajišťující bezpečnost, spolehlivost a udržitelnost.

Příloha č. 4 Pozvánky

Otázky k zodpovězení PTK

Předběžná tržní konzultace ve věci plánované veřejné zakázky na "Mobilní kontejnerové datové centrum" a „Realizace systému zabezpečeného úložiště v prostředí Správy železnic"

V rámci předběžné tržní konzultace bychom Vás požádali o odpovědi a komentáře k následujícím oblastem, předpokládanému průběhu plnění budoucí zakázky/zakázek a předběžným funkčním požadavkům na Mobilní kontejnerové datové centrum a Realizaci systému zabezpečeného úložiště v prostředí Správy železnic, státní organizaci (dále jen „***SŽ***"). Specifikace předmětu plnění je Přílohou č. 2 a Přílohou č. 3 Pozvánky k PTK, které obsahují předběžné požadavky na řešení. **Je nutné se s přílohami č. 2 a č. 3 seznámit před zodpovídáním dotazů v této příloze.**

Dotaz 1	**Vaše odpověď**
Prosíme o vyplnění níže uvedených údajů: • název dodavatele a sídlo dodavatele, • IČO dodavatele, • jméno a funkce kontaktních osob, včetně kontaktních údajů (minimálně e-mail).	

Oblast Technického řešení

Cílem realizace zakázky/zakázek je pořízení komplexního řešení bezpečného datového úložiště pro Správu železnic, které bude realizováno formou mobilního kontejnerového datového centra. Toto řešení zahrnuje dodávku samotného mobilního datového centra (kontejneru), jeho vnitřního vybavení (servery a disková pole) a nadřazeného softwarového systému pro správu, ukládání a archivaci dat.

Mobilní kontejnerové datové centrum bude koncipováno jako samostatný technický modul, vybavený kompletní infrastrukturou pro provoz IT technologií, včetně rackových skříní, redundantního napájení, klimatizace, bezpečnostních systémů a požární ochrany. Konstrukce kontejneru umožní jeho opakovaný transport a instalaci v různých lokalitách, což zajistí provozní kontinuitu i v případě krizových situací, jako jsou přírodní katastrofy, válečné konflikty nebo jiné mimořádné události.

Detailní specifikace kontejneru je uvedena v Příloha č. 2 – Technická specifikace předmětu plnění – Mobilní kontejnerové datové centrum.

Součástí řešení bude rovněž dodávka vybavení do druhé, již existující, geograficky oddělené (geo-redundantní) lokality, která bude sloužit jako záložní datové centrum. Obě lokality budou vzájemně propojeny vysokorychlostní datovou linkou, která zajistí plynulou, bezpečnou a efektivní komunikaci mezi nimi, včetně možnosti replikace dat a automatického přepnutí provozu v případě výpadku jedné z lokalit.

Uvnitř kontejneru budou umístěny servery a disková pole, které budou tvořit samotné datové úložiště. Architektura řešení bude navržena s důrazem na vysokou dostupnost, škálovatelnost, geografickou redundanci a možnost replikace dat mezi oddělenými lokalitami. Úložiště bude schopné pojmout datový

Správa železniční dopravní cesty, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.szdc.cz

Správa železniční telematiky
V Celnici 1028/10
110 00 Praha 1

objem v řádu jednotek petabajtů a bude navrženo tak, aby splňovalo požadavky na retenci a archivaci dat v souladu s bezpečnostními a legislativními předpisy.

Nad hardwarovou vrstvou bude provozován softwarový systém, který zajistí správu datového úložiště, včetně příjmu, zpracování, archivace a řízení životního cyklu dat z různých průmyslových systémů. Bezpečnostní architektura bude zahrnovat šifrování dat při přenosu i při uložení, správu šifrovacích klíčů prostřednictvím HSM, auditovatelnost přístupů a granularitu oprávnění na základě definovaných rolí. Přístupová oprávnění budou řízena centrálně pomocí IDM a PAM, s podporou vícefaktorové autentizace (MFA) a jednotného přihlášení (SSO).

Detailní specifikace bezpečného datového úložiště je uvedena v příloze č. 3 Pozvánky – *Technická specifikace předmětu plnění – Realizace systému zabezpečeného úložiště v prostředí Správy železnic.*

Celé řešení – tedy kontejner, servery a disková pole, softwarová vrstva i integrační prvky – může být předmětem jedné veřejné zakázky. Dotazy v rámci předběžné tržní konzultace (PTK) se vztahují ke všem těmto komponentám a směřují k ověření technických, provozních, bezpečnostních, legislativních a obchodních aspektů navrhovaného řešení.

Tímto komplexním přístupem bude dosaženo cíle aktivity – vytvoření bezpečného, flexibilního a vysoce dostupného úložiště, které bude plně integrováno do bezpečnostní architektury organizace a připraveno na provoz i v krizových podmínkách.

Obecné dotazy

Kapitola obsahuje dotazy vztahující se ke všem částem řešení – kontejneru, hardware i softwaru. Pokrývají celkové pořízení, legislativní soulad, náklady a zkušenosti dodavatele.

Pořízení a implementace

Kapitola zjišťuje formu dodávky, spolupráci na dokumentaci a testování řešení.

Dotaz 2	**Vaše odpověď**
Je pro Vás přiložená technická specifikace předmětu plnění (Příloha č. 2 a č. 3) srozumitelná? Pokud ne, uveďte, proč a co je potřeba doplnit či upřesnit.	ANO / NE / ČÁSTEČNĚ
Váš komentář k zadání.	

Dotaz 3	**Vaše odpověď**
Uveďte prosím všechny kapitoly z Technických specifikací a jejich části, které nejste schopni splnit, případně uveďte důvod. Např. „4.5 Testovací provoz a pilot“.	

Dotaz 4	Vaše odpověď
Nabízíte dodávku řešení formou „na klíč" včetně kontejneru, IT hardware, software, služeb, zabezpečení a následné podpory? V případě částečného plnění, uveďte, kterou část/i jste schopný realizovat.	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 5	Vaše odpověď
Je možné rozdělit dodávku na části (např. zvlášť hardware, zvlášť integrační služby)?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 6	Vaše odpověď
Zajišťujete instalaci mobilního kontejnerového datového centra v lokalitě zákazníka?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 7	Vaše odpověď
Poskytujete součinnost při testování řešení před spuštěním do produktivního provozu? Uveďte příklady Vámi poskytované součinnosti při implementaci dodávky.	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 8	Vaše odpověď
Je možné po dodavateli požadovat spolupráci na úpravě interní dokumentace zadavatele (např. směrnice, metodiky, politiky)? Uveďte konkrétní technologické (vybavení kontejneru) a SW (IdM, DLP, XDR) oblasti Vaší možné součinnosti.	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 9	Vaše odpověď
Jaká je nejkratší předpokládaná doba dodání díla od podpisu smlouvy? Uveďte dobu dodání včetně instalace a uvedení do provozu. V případě částečného plnění (kontejner/zabezpečené úložiště) uveďte dobu dodání za každou takovou část.	
Váš komentář k navrhovanému řešení.	

Dotaz 10	Vaše odpověď
Jakou byste navrhoval architekturu zabezpečení komunikace vámi dodávaného bezpečného úložiště, aby byla v souladu s technickou specifikací (prosím uveďte popis nebo high level diagram)?	
Váš komentář k navrhovanému řešení.	

Legislativa a veřejná zakázka

Kapitola ověřuje soulad s právními předpisy, zkušenosti s veřejnými zakázkami.

Dotaz 11	Vaše odpověď
Máte zkušenosti s veřejnými zakázkami v oblasti kritické infrastruktury?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 12	Vaše odpověď
Splňuje řešení požadavky zákona o kybernetické bezpečnosti (ZoKB) 264/2025 Sb. a vyhlášky o kybernetické bezpečnosti (VoKB) 409/2025 Sb.? Jaké certifikace nebo audity to dokládají?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 13	Vaše odpověď
Máte praktické zkušenosti s projektu pro klienta, na kterého se vztahuje ZoKB 181/2014 Sb. a VoKB? Pokud ano, stručně je popište.	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 14	Vaše odpověď
Dle jakých norem (ISO, EN, ČSN) je řešení navrhováno? Rozepište prosím dle jednotlivých kategorií (elektro, fyzická bezpečnost, požární bezpečnost a další)?	

Náklady

Kapitola mapuje možnosti financování, rámcové ceny a výpočet celkových nákladů vlastnictví.

Dotaz 15	Vaše odpověď
Jaká je orientační cena plnění za část „Mobilní kontejnerové datové centrum“? Prosíme o předložení cenového rozpadu.	

Dotaz 16	Vaše odpověď
Jaká je orientační cena plnění za část „Realizace systému zabezpečeného úložiště v prostředí Správy železnic“? Prosíme o předložení cenového rozpadu.	

Dotaz 17	Vaše odpověď
Byla by cena v případě dodání obou částí (kontejner + IT vybavení) pro zadavatele výhodnější? Uveďte předpokládanou cenu celkového plnění. Prosíme o předložení cenového rozpadu.	

Dotaz 18	Vaše odpověď
Nabízíte možnost pořízení formou jednorázové investice (CapEx)?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 19	Vaše odpověď
Nabízíte možnost pořízení formou průběžných plateb (OpEx)?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 20	Vaše odpověď
Je možné získat rámcový ceník nebo ukázkovou konfiguraci s cenou? Pokud ano, uveďte prosím odkaz k nahlédnutí či stažení.	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 21	Vaše odpověď
Lze odhadnout provozní náklady řešení na 1 rok, 5 let a 10 let dopředu? Pokud ano, uveďte prosím částku.	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 22	Vaše odpověď
Jaká je předpokládaná životnost jednotlivých technologií? • kontejner + podpůrné technologie • data storage, servery	
Váš komentář k navrhovanému řešení.	

Dotaz 23	Vaše odpověď
Nabízíte model TCO výpočtu pro různé varianty konfigurace?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Reference a zkušenosti

Kapitola se zaměřuje na předchozí realizace, technické kompetence a schopnost provozní podpory.

Dotaz 24	Vaše odpověď
Dodávali jste v posledních 3 letech obdobné řešení jiným subjektům?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 25	Vaše odpověď
Uveďte prosím seznam vašich relevantních projektů v oblasti kontejnerového řešení a zabezpečeného úložiště včetně stručného popisu předmětu dodávky/služby.	

Dotaz 26	Vaše odpověď
Uveďte seznam vašich relevantních projektů v oblasti kritické infrastruktury (KII) včetně stručného popisu předmětu dodávky/služby.	

Dotaz 27	Vaše odpověď
Máte zkušenosti s integrací HSM a IDM? Uveďte konkrétní příklady včetně stručného popisu předmětu dodávky/služby.	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 28	Vaše odpověď
Máte zkušenosti s integrací XDR od výrobce Fidelis?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 29	Vaše odpověď
Uveďte příklady vašich projektů, jejichž předmětem byla dodávka mobilního datového centra s minimální diskovou kapacitou 3 petabajtů, včetně provozní podpory (SLA). Uveďte typy provozní podpory, které jste schopni nabídnout.	

Dotaz 30	Vaše odpověď
Máte zkušenosti s migrací dat v rozsahu petabajtů? Jaké nástroje jste použili?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 31	Vaše odpověď
Uveďte příklady vašich projektů s geografickou redundancí a disaster recovery včetně stručného popisu předmětu dodávky/služby.	

Dotaz 32	Vaše odpověď
Poskytujete školení a dokumentaci v českém jazyce?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 33	Vaše odpověď
Máte k dispozici náhled vzorového řešení? Například vzorový kontejner na ukázku nebo zprostředkovaná návštěva za účelem prohlídky kontejneru u zákazníka. Případně byla by možná návštěva Vašeho výrobního závodu?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Vaše další komentáře k této PTK

V případě, že považujete za vhodné nám sdělit Vaše další komentáře nebo doporučení k předmětu této PTK nebo možným budoucím veřejným zakázkám s PTK spojených, prosíme o vaše další vyjádření níže:

Vaše další komentáře k předmětu PTK