Příloha č. 2 Smlouvy o dodávce a implementaci informačních a komunikačních technologií

Technické požadavky Objednatele

Obsah

1. Systém řízení kontinuity provozu (BCM) – popis očekávaného řešení, stavu a potřeb Objednatele

Záměrem Objednatele je zavést systém řízení kontinuity provozu (Business Continuity Management, dále jen „BCM"), jehož cílem je posílit schopnost Objednatele reagovat na mimořádné a krizové situace a zároveň minimalizovat dopady na klíčové činnosti, služby a informační infrastrukturu. Výsledné řešení musí být stabilní, prakticky využitelné a začlenitelné do běžného provozního prostředí multifunkční haly.

Objednatel požaduje realizaci systému BCM, který umožní:

- identifikaci a kategorizaci **klíčových činností a aktiv**, včetně vazeb mezi primárními a podpůrnými aktivy,
- definování **minimální úrovně funkčnosti** (Level of Business Continuity) v případě jejich narušení,
- stanovení parametrů obnovy, jako jsou:
    - **RTO (Recovery Time Objective)** – maximální přípustná doba obnovení činnosti,
    - **RPO (Recovery Point Objective)** – maximálně akceptovatelná ztráta dat,
        - Hodnoty RTO, RPO a MTO budou stanoveny na základě výsledků předimplementační analýzy (BIA a technického posouzení), s přihlédnutím k reálným možnostem stávající i cílové HW/SW infrastruktury a architektury systémů. V této fázi dokumentu jsou uvedeny pouze metodické principy jejich stanovení.
    - **MTO (Maximum Tolerable Outage)** – maximální tolerovatelná doba narušení činnosti, po kterou jsou dopady pro organizaci ještě akceptovatelné,
    - **MBCO (Minimum Business Continuity Objective)** – minimální úroveň poskytování služby v režimu kontinuity,
- vyhodnocení relevantních **rizik a dopadů** prostřednictvím analýzy dopadů na činnost (BIA), včetně hodnocení vývoje těchto dopadů v čase a definice priorit obnovy,
- předložení **Plánu kontinuity podnikání (BCP)** jako komplexního dokumentu zahrnujícího:
    - plán reakce na incidenty (IRP),
    - plán obnovy po havárii (DRP),
    - plán náhradního provozu,
    - plán krizové komunikace (interní i externí),
    - postupy eskalace a rozhodování,

    - definici náhradních pracovišť a záložních zdrojů,
    - plán přechodu k normálnímu provozu po ukončení krizové situace,
- začlenění BCM do běžného provozu včetně propojení s dalšími systémy a procesy organizace.

Součástí zvoleného řešení bude dále:

- jasná definice rozhodovacích pravomocí a rolí klíčových osob v případě krizových situací, včetně ustanovení zástupců,
- stanovení způsobu včasného a jednoznačného informování interních týmů během mimořádných událostí,
- postupy krizového řízení a svolávání týmů dle eskalační matice,
- zohlednění spolupráce s třetími stranami včetně identifikace klíčových smluvních vztahů, dodavatelů a externích služeb (včetně podstatných detailů smluvních ustanovení),
- přehled potřebného technického zázemí (hardware, software, síťové a zálohovací prostředky, komunikační zařízení) nutného k obnovení činnosti, včetně uživatelských manuálů,
- určení vhodných náhradních míst nebo nouzových pracovišť, kde je možno pokračovat v činnostech, včetně vysvětlení přístupu k nim,
- seznam všech rozhodujících dokumentů (listinných i elektronických) a postupy jejich obnovy,
- funkční metodiku testování, školení a pravidelné aktualizace plánů, včetně:
    - metodiky a scénářů pro testování připravenosti (desktop exercises, simulace, full-scale testy),
    - základního školení klíčových osob tak, aby byli schopni udržovat danou dokumentaci aktuální,
    - doporučení k provádění krizových cvičení,
    - metodiky vyhodnocování testů a implementace poznatků (lessons learned),
- dostupnost plánů včetně off-line verzí pro případ výpadku ICT infrastruktury (tištěné nebo na off-line médiích),
- začlenění do procesu řízení změn a návaznost na interní organizační struktury a provozní odpovědnosti,
- integrace s ICT službami a organizační strukturou.

Objednatel požaduje, aby řešení:

- bylo v souladu s požadavky normy **ISO/IEC 22301**,
- respektovalo požadavky **zákona č. 264/2025 Sb., o kybernetické bezpečnosti**, ve znění pozdějších předpisů,
- přihlíželo k doporučením a varováním **NÚKIB**,

- zahrnovalo návrh školení a krizových cvičení včetně zapojení vedoucích pracovníků a klíčových útvarů organizace,
- umožňovalo dlouhodobou udržitelnost, provozní přenositelnost a praktické využití v různých režimech provozu organizace.

Implementace a provozní požadavky

Důraz je kladen na to, aby Zhotovitelem zvolené řešení bylo reálně implementovatelné v podmínkách konkrétního provozu Objednatele. Plány musí být srozumitelné, jednoznačné a snadno aktivovatelné i v krizové situaci, kdy může být dostupnost zdrojů omezená.

Objednatel dále očekává, že v rámci řešení budou zohledněny skutečné provozní priority a specifika prostředí multifunkční haly, včetně scénářů výpadků energií, ICT, přístupových systémů nebo lidských zdrojů.

Předpokládá se aktivní spolupráce s Objednatelem při definici krizových rolí a při tvorbě i schvalování klíčových dokumentů.

Kontinuální zlepšování a udržitelnost

Zvláštní důraz je kladen na zajištění praktického testování připravenosti, jehož výstupy budou sloužit jako zpětná vazba pro další úpravy plánů. Klíčové je, aby BCM nebylo jednorázovým projektem, ale živým systémem s pravidelnou aktualizací, návazností na změny v provozu a schopností dlouhodobé adaptace, včetně:

- procesu pravidelného přezkoumání BCM,
- metodiky pro dokumentování a vyhodnocování poznatků z testů i reálných incidentů,
- procesu aktualizace BIA při významných změnách v organizaci,
- stanovení frekvence a rozsahu aktualizací jednotlivých plánů,
- zajištění neustálého zlepšování systému.

Cílem je dosáhnout stavu, kdy bude Objednatel schopen reagovat na krizové situace koordinovaně, informovaně a včas, s minimalizací dopadů na provoz, zaměstnance i veřejnost.

Pravidelné aktualizace a údržba BCM budou zařazeny do oblasti rozvoje a udržitelnosti systému. Případné drobné úpravy a změny (v rozsahu časové náročnosti max. 1 hod.) budou realizovány na základě incidentů řešených v rámci provozní podpory.

2. Služby implementace systému správy identit (IDM) – popis požadovaného řešení, stavu a potřeb Objednatele

Objednatel požaduje implementaci a provoz systému správy identit (IDM), který bude sloužit jako centrální nástroj pro řízení digitálních a fyzických oprávnění osob pohybujících se v prostředí multifunkční haly ARENA BRNO. Řešení musí zahrnovat správu interních i externích identit, jejich životní cyklus a automatizaci procesů napříč IT a provozní infrastrukturou.

Cílem je:

- zajištění centralizované a auditovatelné správy identit napříč celým prostředím Objednatele,
- vytvoření trvale udržitelného a provozně efektivního řešení pro řízení přístupových oprávnění,
- podpora provozních scénářů s vysokou dynamikou změn (např. hromadné akce, sportovní či kulturní události),
- integrace IDM s provozními, bezpečnostními a IT systémy (včetně elektronické kontroly vstupu, docházky a dalších).

Systém musí reflektovat rozdílné potřeby různých kategorií osob pohybujících se v prostředí haly. Kromě kmenových zaměstnanců a externích pracovníků účastnících se krátkodobých nebo jednorázových akcí může systém pokrývat rovněž správu identit pro VIP návštěvníky, akreditované novináře, mediální týmy a další dočasné subjekty s časově omezeným nebo událostně podmíněným přístupem. Zhotovitel je povinen předložit návrh a realizovat řešení s jasnou segmentací a technickým řešením pro zmíněné skupiny uživatelů, včetně mechanismů pro rychlou registraci, přidělení oprávnění a jejich automatické odvolání po skončení akce.

1. Segmentace identit a požadavky na řešení

1.1 Kmenoví zaměstnanci (cca 50 osob)

Identita a správa:

- Trvalá identita spravovaná v Active Directory nebo Azure AD či ekvivalentu
- Napojení na IDM přes LDAP, nebo prostřednictvím OIDC/SAML/MS Graph API v případě využití Azure AD (Entra ID)
- Správa životního cyklu uživatele (onboarding, změny, offboarding)

Autentizace a autorizace:

- Autentizace: Active Directory či ekvivalent
- Možnost vícefaktorové autentizace (MFA) – např. mobilní aplikace, token

- Autorizace: Řízená přes systém IDM na základě rolí a organizační struktury s využitím AD
- Automatizace oprávnění dle role

Přístupové systémy a integrace:

Zhotovitel musí navrhnout a realizovat IDM řešení s možností integrace přístupu kmenových zaměstnanců k následujícím systémům:

- **Firemní Wi-Fi síť** (RADIUS + AD, 802.1x)
- **Ethernetová síť (LAN)** (802.1x + AD)
- **Tiskárny** (AD-based access)
- **Lokální úložiště** (NAS, SharePoint, OneDrive nebo obdobné)
- **Docházkový systém**
- **ERP systém – pokud bude později doplněn**
- **Stravovací systém**
- **Elektronická kontrola vstupu (EKV)**
- **Parkoviště a garáže** (RFID/QR přístup)

Objednatel, bez ohledu na výše popsané systémy, které jsou předmětem samostatných řízení, předpokládá komunikaci prostřednictvím standardizovaných protokolů. V současné době nemá Objednatel dokončený proces výběru dodavatelů u uvedených systémů; stanovuje pouze požadavek na standardizovanou a otevřenou formu komunikace.

Badge systém, karta/Token:

- Karta / Token napojená skrze IDM na Active Directory či ekvivalent, např. z důvodu přihlášení k PC
- Karta / Token může sloužit jak pro fyzický, tak i logický přístup
- Formát: Podle požadavků Objednatele (RFID, QR kód, případně kombinace)
    - RDIF
        - **Pro EKV** - Dodavatel zajistí možnost napojení a kompatibility na standardizovanou čtečku **RFID karet Elatec TWN4, kterou dodá Objednatel skrze čtečky Dodavatele EKV (společnost Trade FIDES a.s.)**
    - **Badge s QR kódem**
        - Vazba: QR kód jako unikátní identifikátor napojený na záznam v IDM a umožňující rozšíření vstupu a kontroly pro EKV
        - Doporučený formát: QR kód + fotografie + jméno + ID
- Bezpečnost: Bezpečnostní podpis obsahu badge

Audit:

- Všechny operace logovány v systému IDM
- Možné napojení na SIEM Dodavatele

- Logování změn oprávnění a přístupů

Důvod vedení v AD: - Kmenoví zaměstnanci jsou vedeni v Active Directory či ekvivalentu z následujících důvodů: tvoří trvalou součást IT prostředí Objednatele, vyžadují přístup k více systémům současně, jejich správa podléhá požadavkům na audit a komplexní řízení oprávnění a jejich identity jsou integrovány s firemními ICT službami.

1.2 Externí pracovníci (desítky až stovky dle akce), případně novináři a VIP

Identita a správa:

- Evidence v samostatné databázi systému IDM (mimo Active Directory či ekvivalent)
- Časově omezená platnost identity a oprávnění
- Automatické ukončení oprávnění po vypršení časové platnosti
- Role-based přístup (např. technik, promotér, personál akce, VIP zákazník, externí pracovník)

Autentizace a autorizace:

- Autentizace: QR badge s fotografií nebo RFID Kartou
- Zrychlení validace a ověření:
- **Zajištění kompatibility se standardizovanými doklady totožnosti vydanými v EU (občanské průkazy, pasy)**
    - Typ kompatibilní čtečky dokladů je specifikuje Zhotovitel v rámci předimplementační analýzy
    - Dodávka čteček není předmětem plnění Zhotovitele. Zhotovitel zajistí technickou kompatibilitu a připravenost řešení tak, aby Objednatel mohl čtečky dodatečně objednat dle aktuální potřeby.
- Autorizace prostřednictvím standardizovaných protokolů:
    - **OAuth 2.0** (autorizace)
    - **OpenID Connect** (autentizace)
    - **JWT (JSON Web Token)** pro přístup do cílových systémů
- Možnost využití federované identity prostřednictvím standardního OpenID Connect providera

Tok autentizace a autorizace:

Zhotovitel musí zajistit následující proces:

1. Externí pracovník se registruje v portálu (např. portál pro promotéry)
2. Přes REST API nebo jiné integrační rozhraní bude automaticky importován do systému IDM
3. Systém IDM rozšíří oprávnění na základě předem definovaných konfigurovatelných šablon (business rolí)

4. Business role na základě hodnot atributů uživatele automaticky rozšíří oprávnění (např. přístup ke konkrétním vstupům, sekcím, parkovišti)
5. Rozšířená oprávnění mohou být na definovanou dobu přiřazena i manuálně správcem IDM
6. Systém, pokud tak Zhotovitel rozhodne, vystaví skrze pověřené pracovníky přístupový token (např. JWT) na základě přihlášení
7. Token je předán cílovému systému (např. EKV), který ověří oprávnění
8. Přístup je udělen na základě role, časového omezení a typu akce

Import a správa:

- Hromadný import externích pracovníků z CSV, XML, Excel
- Ruční zadání přes webové rozhraní
- Automatické vyhledávání a identifikace již známého uživatele
- Možnost kontejnerizace (skupiny) uživatelů dle akcí

Přístupové systémy:

Externí pracovníci budou (VIP či akreditovaní novináři mohou) mít přístup k omezenému rozsahu systémů, např.:

- **Elektronická kontrola vstupu (EKV)** – vstupy, sekce, zázemí
- **Parkoviště a garáže**

Externí pracovníci **nebudou mít primárně určený přístup** k interním ICT službám krom možného přístupu k Wi-Fi či Tiskárnám. Konkrétní přistup a segmentace bude upřesněna a nastavena v předimplementační analýze.

Externí portál pro promotéry a správce akcí:

Zhotovitel musí zajistit webové rozhraní (portál) pro správu externistů s následujícími funkcemi:

- **Registrace akcí** – vytvoření události, definice rolí
- **Import externistů** – hromadný import nebo ruční zadání
- **Správa oprávnění** – výběr sekcí, časové okno, typ přístupu
- **Generování badge** – tisk nebo export QR kódů s fotografií
- **Monitoring** – přehled přístupů, auditní logy, export dat
- **Oddělené prostředí** pro externí správu – pro promotéry, externí garanty služeb (např. security)
- **Možnost záložního režimu** – portál IDM může v případě výpadku externího portálu plnit funkci nástroje pro hromadný import

Validace identity a vydání karty, badge:

- Při akreditaci může nastat situace, kdy je Badge karta vydána na základě předloženého identifikačního dokladu. Doklad je načítán prostřednictvím čtečky dokladů za účelem urychlení vyhledání příslušné osoby v systému a zároveň slouží k ověření její identity.
- Pro zrychlení práce obsluhy během akreditace může být centrálně využíváno prostředí IDM v komunikaci se systémem EKV, a to v následujícím postupu:
    - Daná osoba je identifikována prostřednictvím čtečky dokladů nebo předložením dokladu:
        - na základě předchozího založení záznamu (např. importem před zahájením akce), nebo
        - během akreditace přímo na místě.
    - Osoba je v systému IDM zařazena do příslušné skupiny.
    - Na základě přiřazené skupiny jsou do dotčených systémů odeslána oprávnění, přístupy a nastavení chování.
    - Probíhá komunikace s čtečkou RFID karet za účelem zápisu datové věty dané osoby pro potřeby EKV.
    - Probíhá vygenerování QR kódu (například pro přístup k Wi-Fi, tiskárnám) který může být později rozšířen i o identifikaci pro EKV (v současnosti ale nejsou dveřní čtečky vybaveny čtením QR kódů).
    - Dochází k tisku Badge karty ve formátu odpovídajícím dané akci a k předání RFID karty.

Vztah IDM vs EKV

Objednatel upozorňuje, že konkrétní způsob komunikace s EKV, čtečkou RFID karet, tisk Badge karet i finální nastavení procesu může být upřesněno po dohodě s Dodavatelem EKV (společností Trade FIDES a.s.) v předimplementační analýze, zejména pokud jde o to, ze kterého prostředí bude probíhat zápis na RFID kartu a tisk Badge karet.

Z hlediska architektury platí, že systém IDM vystupuje jako autoritativní zdroj identit a oprávnění. Systém EKV přijímá oprávnění z IDM a vykonává fyzickou kontrolu vstupu. Konkrétní způsob předávání těchto oprávnění mezi oběma systémy bude stanoven v předimplementační analýze.

Pro Dodavatele je podstatné, že musí být schopen pracovat s čtečkou RFID karet Elatec TWN4, tisknout Badge karty včetně podpory QR kódů a načítat doklady prostřednictvím čtečky dokladů. Záměrem Objednatele je, aby během akreditace nedocházelo na straně obsluhy k využívání více systémů pro odbavení dané osoby — veškeré kroky by tedy měly být dostupné a proveditelné z jednoho prostředí.

1.3 Běžný návštěvník

Je odbaven na základě vstupenky, tiketovacího odbavovacího systému (není předmětem plnění Zhotovitele). Nebude tak veden v IDM či AD z důvodu nákladnosi licencí (např. CAL) ,

administrativní zátěži, nepotřebě přístupu k ICT službám a z důvodu vysoké fluktuace a krátkodobost přístupů

2. Funkční požadavky na systém IDM

2.1 Správa identit a oprávnění

- **Snadná správa** pro interního správce i externího správce pro danou akci
- **Evidence všech rolí**, oprávnění a vstupů zaměstnanců a externistů včetně přidělených oprávnění
- **Kontejnery (skupiny) uživatelů** dle akcí
- **Automatické vyhledávání a identifikace** již známého uživatele
- **Možnost tvorby pravidel** v uživatelském prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí na základě kombinace atributů identity
- **Možnost přehledné správy referenčních objektů** (systematizované místo, organizační jednotka, skupina, aplikace, aplikační role, certifikát atd.)
- **Možnost grafického zobrazení identit** ve stromové organizační struktuře
- **Možnost přikládat k jednotlivým účtům obrázky** (fotografie)
- **Možnost sjednocení více identit** do jedné a odpovídající sjednocení spravovaných účtů
- **Možnost zabránění hromadným změnám** z důvodu případných chybných vstupních dat

2.2 Workflow a schvalování

- **Možnost automatizace** včetně procesního schvalování oprávnění
- **Konfigurovatelná workflow** pro schvalování vytvoření objektů a vazeb, plánované akce
- **Samoobslužné uživatelské rozhraní** pro zadávání žádostí o přidělení jednotlivých aplikačních rolí a členství ve skupinách
- **Kategorizace rolí a skupin** s možností přidělit schvalovací workflow nebo automatické vyřízení

2.3 Notifikace

- **Automatické e-mailové notifikace** s možností konfigurace obsahu, adresátů a podmínek
- **Možnost tvorby notifikačních šablon** a definice příjemce, předmětu a obsahu upozornění
- **Alertování veškerých změn** a atributů v systému včetně nastavování upozornění (např. upozornění na vypršení hesla)

2.4 Životní cyklus identit

- **Správa životního cyklu identit**, aplikací, aplikačních a business rolí (založení, změna, zakázání, smazání)
- **Automatické i manuální přiřazování rolí** s možností nastavení časové platnosti
- **Možnost přiřazení rolí** konkrétní identitě, pracovnímu místu, skupině a organizační jednotce včetně data a času vypršení platnosti
- **Automatické odebrání role** po vypršení platnosti přiřazení
- **Možnost přiřazení identit** k pracovním místům a organizacím ve vazbě M:N
- **Správa skupin** s možností začleňovat více skupin do sebe, přiřazovat jednotlivé uživatele i pracovní místa

2.5 Audit a monitoring

- **Evidence a archivace** poskytnutých oprávnění, včetně přehledu, na co jsou role a oprávnění navázané
- **Logování a monitoring veškerých změn** oprávnění, včetně exportu logů mimo dosah administrátorů IDM
- **Auditní logy** s možností napojení k SIEMu Zhotovitele
- **Transakční provádění změn** s logováním původní i nové hodnoty
- **Možnost u identity zobrazit seznam všech rolí** včetně informace, odkud uživatel roli zdědil

3. Technické požadavky

3.1 Integrace a konektory

Zhotovitel musí zajistit integraci s následujícími systémy prostřednictvím standardizovaných rozhraní, a to zejména v rozsahu (může být upřesněn dle definování přístupových rolí):

- **Active Directory** – synchronizace identit, oprávnění (LDAP, Kerberos)
- **Personální systém** – jako zdrojový systém pro import kmenových zaměstnanců
- **Docházkový systém** – korelace přístupů s reálnou docházkou
- **ERP** – přístupová práva, role
- **EKV** – fyzický přístup dle oprávnění
- **Tiskové služby** – přístup k tiskovým službám
- **Wi-Fi / LAN** – síťový přístup (RADIUS, 802.1x)
- **Stravovací systém**
- **Parkovací systém**

Požadované typy konektorů:

- **Vestavěné obecné skriptovatelné konektory** minimálně v tomto rozsahu:
    - Konektor pro spouštění CMD a PowerShell příkazů, SSH

- Konektor pro práci s CSV soubory
- Konektor pro práci s databází Microsoft SQL, Oracle
- Konektor pro napojení na SOAP webové služby
- Konektor pro napojení na REST webové služby
- Konektor pro LDAP
- Podpora dalších standardizovaných protokolů (SAML, OpenID Connect, OAuth 2.0)

3.2 Režimy synchronizace

Systém musí podporovat následující režimy synchronizace s integrovanými systémy:

- **Plná synchronizace** – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému
- **Změnová synchronizace** – synchronizuje vždy jen změny od poslední spuštěné synchronizace
- **Okamžitá synchronizace** konkrétní identity na vyžádání
- **Rekonciliační synchronizace** – vytvoří report pro porovnání změn mezi IDM a připojeným systémem
- **Simulační synchronizace** – vytvoří report očekávaných změn bez ovlivnění produkčních dat
- **Sekvenční synchronizace** – spouštění synchronizací v sekvencích s možností automatického i ručního spuštění
- **Ruční i automatické spuštění synchronizací** s možností definovat agenty pro plánované úlohy

3.3 Bezpečnostní opatření

- **OAuth 2.0 + OpenID Connect** – standardizované, bezpečné protokoly pro autentizaci/autorizaci externích pracovníků
- **JWT tokeny** – expirace, podpis, krátká doba platnosti s podporou refresh tokenů
- **Vícefaktorová autentizace (MFA)** pro kmenové zaměstnance
- **Šifrování dat** v klidu i přenosu (TLS, AES)
- **Segmentace přístupů** (interní vs. externí)
- **Role-based access control (RBAC)**
- **Soulad s legislativou** – GDPR, NIS2, Zákon o kybernetické bezpečnosti
- **Validace identity** – OP/pas/eDoklady

3.4 Uživatelské rozhraní

- **Webové rozhraní** (podpora moderních prohlížečů – zejm. MS Edge, Firefox, Chrome)
- **Vícejazyčná podpora (český, anglický jazyk)**
- **Řízení přístupu** dle aplikačních rolí

- **Změna/reset hesla**
- **Logování změn**
- **Možnost převzetí správy** při výpadku zdrojových systémů

4. Technické komponenty a licenční model

Zhotovitel musí v rámci předimplementační analýzy specifikovat zvolené řešení a toto řešení následně realizovat:

4.1 Hardware a software požadavky

- **A)**
    - **Specifikace HW** pro řešení (CPU, RAM, HDD, počet serverů) v závislosti na počtu spravovaných identit (500-5000 uživatelů)
        - Napojení a kompatibilita se čtečkou dodavatele EKV (Trade FIDES, a.s.) a Elatec TWN4 dodanou Objednatelem
        - Kompatibilita se standardizovanou čtečkou dokladů totožnosti vydanými v EU (občanské průkazy, pasy) specifikovanou Zhotovitelem v rámci předimplementační analýzy
            - Dodávka čteček není předmětem plnění Zhotovitele. Zhotovitel zajistí technickou kompatibilitu a připravenost řešení tak, aby Objednatel mohl čtečky dodatečně objednat dle aktuální potřeby; Zhotovitel je povinen poskytnout Objednateli nezbytné informace, aby toto dodatečné objednání bylo proveditelné.
    - **Specifikace SW** (operační systém, databáze, middleware)
    - **Licence třetích stran** (Windows Server, SQL Server, Active Directory, SQL CAL, AD CAL apod.)
- B)
    - Využití virtualizace
- C)
    - Využití cloudového nasazení

4.2 Licenční model

- Použitý licenční režim (perpetual/subscription)
- Přehled omezení a dopadů při přerušení licence nebo údržby (maintenance)
- Cenová politika pro škálování (přidání uživatelů, modulů)
- Licence a maintenance systému IDM umožňující instalaci a upgrade systému

5. Implementační analýza a konzultační podpora

Součástí předimplementační analýzy bude:

5.1 Analýza a návrh

- Odborná analýza struktury uživatelů, provozních rolí a přístupových scénářů
- Návrh instalace a parametrizace systému
- Návrh integrační topologie a správy oprávnění dle typu uživatele
- Návrh implementace integrací na všechny požadované systémy
- Detailní popis procesů realizovaných v systému IDM
- Detaily způsobu integrace systému IDM na zdrojové a cílové systémy

5.2 Implementace a školení

- Implementace workflow pro životní cyklus identit
- Podpora scénářů pro hromadnou správu (např. importy externích osob pro akce)
- Implementace krizových scénářů (např. evakuace, výpadky)
- Školení administrátorů a provozního personálu
- Dokumentace: provozní manuály, bezpečnostní směrnice, metodiky
    - Zejména:
        - Provozní manuály specifické pro oblast IDM
        - Bezpečnostní směrnice a postupy pro správu identit a přístupů
        - Metodiky pro běžný provoz, řešení incidentů a změnové řízení
        - Vstupy pro integraci do celkového KyBe konceptu (bezpečnostní události, monitoring, eskalační postupy)
        - Vstupy pro BCM (postupy obnovy, RTO/RPO, krizové scénáře)

6. Požadavky na součinnost ze strany Objednatele

Zhotovitel v rámci předimplementační analýzy specifikuje nutnou součinnost od Objednatele, a to minimálně v rozsahu:

- Zajištění licencí a maintenance systému IDM
- Zajištění integračních rozhraní požadovaných systémů (Active Directory, Personální systém, ERP, EKV, Docházka, Wi-Fi/LAN, Tisk, Stravovací systém, Parkovací systém)
- Nastavení požadovaných prostupů mezi synchronizační službou IDM a integrovanými systémy
- Vytvoření technických účtů pro instalaci a konfiguraci systému IDM a synchronizačních účtů, včetně nastavení jejich oprávnění pro čtení a zápis dat do integračních rozhraní
- Zajištění kapacit správců integrovaných systémů pro konfiguraci konektorů, testování funkčnosti, migraci uživatelských účtů a jejich oprávnění
- Účast pracovníků Objednatele na školení
- Zajištění potřebných kapacit a kompetencí odpovědných zaměstnanců pro akceptaci výstupů služeb

7. Obecné požadavky na řešení

Řešení musí být navrženo jako otevřená a rozšiřitelná platforma s důrazem na:

- **Standardizovaná rozhraní** (REST API, LDAP, SAML, OpenID Connect, OAuth 2.0)
- **Auditovatelnost všech operací**
- **Podporu vícefaktorové autentizace**
- **Soulad s legislativou GDPR**
- **Provoz v režimu 24/7**
- **Vysokou dostupnost** i při výpadku jednotlivých komponent
    - **Pokud je řešení provozováno ve virtuálním prostředí**, musí být vysoká dostupnost zajištěna prostřednictvím mechanismů a architektury dané virtualizační platformy navrhnuté Zhotovitelem.
    - **Pokud je řešení realizováno formou cloudové služby nebo jako on-premise serverové nasazení mimo virtualizační cluster,** musí Zhotovitel v rámci řešení zohlednit redundanci kritických komponent.
- Škálovatelnost pro podporu proměnlivé intenzity zátěže
- **Provoz i mimo běžné pracovní hodiny**

Řešení musí odpovídat provozním podmínkám multifunkční haly s proměnlivou intenzitou zátěže a potřebou provozu i mimo běžné pracovní hodiny.

3. Kybernetická bezpečnost, organizačně bezpečnostní opatření – popis požadovaného řešení, stavu a potřeb Objednatele

Objednatel očekává návrh postupů, komunikačních mechanismů a provozních pravidel pro zajištění efektivní spolupráce s odborným partnerem v oblasti kybernetické bezpečnosti. Cílem této spolupráce je podpora při návrhu a postupném budování odolného, auditovatelného a dlouhodobě udržitelného bezpečnostního rámce, který bude přizpůsoben specifickému prostředí organizace ARENA BRNO, a.s.

Cílem spolupráce je:

- vyhodnotit a posílit úroveň ochrany informačních aktiv a systémů organizace,
- zajistit soulad s platnou a připravovanou legislativou (zejména NIS2, GDPR, Zákon č. 264/2025 Sb., o kybernetické bezpečnosti), případně realizace dle Best Practice a souvisejících doporučení v situaci, kdy Objednatel nebude povinen dle ZoKB,
- vytvořit strategii a opatření vedoucí k řízenému zvládání kybernetických hrozeb,
- zvýšit odolnost vůči kybernetickým hrozbám,
- vytvořit auditovatelný bezpečnostní rámec,

- posílit připravenost na kybernetické incidenty a schopnost organizace na ně reagovat,
- zajistit odpovídající dokumentaci, procesy a odpovědnosti,
- zajistit metodické a dokumentační zázemí pro bezpečnostní správu a dohled.

Řešení bude plně přizpůsobeno specifickému prostředí multifunkčního objektu a bude reflektovat provozní realitu a technologické možnosti.

1. Hlavní oblasti řešení

Objednatel požaduje návrh a zavedení opatření v následujících oblastech, které budou vzájemně provázané a orientované na praktickou proveditelnost, přenositelnost a udržitelnost:

1.1 Systém řízení bezpečnosti informací (ISMS)

- **Definování základního bezpečnostního rámce a odpovědností**
- **Přiřazení rolí:**
  - Bezpečnostní správce/manažer nebo koordinátor ISMS
  - Schvalovatelé
  - Auditoři
  - Jasné určení odpovědností za bezpečnost informací na všech úrovních organizace
- **Zavedení procesů:**
  - Řízení rizik
  - Řízení aktiv
  - Řízení přístupu
  - Kontrola změn
  - Zajištění kontinuity
- **Vytvoření matice odpovědností (RACI)** pro bezpečnostní procesy
- **Stanovení jednotného vzoru dokumentů**, včetně stanovení odpovědností a povinností pravidelné aktualizace

1.2 Politiky a směrnice

- **Stanovení bezpečnostní politiky**, která definuje cíle, zásady a rámec řízení bezpečnosti informací
- **Vytvoření interních směrnic** pro konkrétní oblasti:
  - Přístupová práva
  - Práce na dálku
  - Nakládání s citlivými daty (ochrana osobních údajů)
  - Klasifikace aktiv
  - Využití vlastních zařízení (BYOD)
  - Bezpečnostní minimum pro pracovní stanice, servery a síťové prvky

- **Pravidla pro nové zaměstnance a externí subjekty**
- **Definování povinností v rámci GDPR** dle jednotlivých procesů a dopadů na subjekty údajů

1.3 Opatření technické a organizační ochrany aktiv

- **Nastavení přístupových pravidel:**
  - Definování pravidel pro přidělování, změnu a odebrání přístupových práv
  - Zavedení principu „nejmenšího potřebného přístupu" (least privilege)
- **Segmentace a řízení privilegovaných účtů**
- **Doporučení k technickým opatřením:**
  - Šifrování
  - Zálohy
  - Vícefaktorové ověřování (MFA)
  - Správa aktualizací
- **Přiřazení odpovědnosti** za ochranu jednotlivých typů aktiv

1.4 Klasifikace aktiv a řízení rizik

- **Zjednodušená klasifikace aktiv** dle:
  - Důvěrnosti
  - Dostupnosti
  - Integrity
- **Identifikace, hodnocení a řízení rizik** spojených s informačními aktivy
- **Rámcový postup hodnocení rizik** a výběru adekvátních opatření
- **Definice role vlastníka aktiva** a způsobu správy rizik
- **Zavedení procesů** pro pravidelné přezkoumání a aktualizaci rizik
- **Návrh přiměřených opatření** pro jejich eliminaci nebo zmírnění

1.5 Struktura bezpečnostní dokumentace a její správa

- **Katalog bezpečnostních dokumentů:**
  - Politika
  - Směrnice
  - Postupy
- **Návrh šablon, verzování, revizní postup**
- **Jasné určení schvalovacích a publikačních odpovědností**

1.6 Řízení a reakce na incidenty

- **Vytvoření plánu reakce na bezpečnostní incidenty**
- **Základní proces zvládání incidentů:**
  - Detekce

    - Eskalace
    - Reakce
    - Vyhodnocení
- **Zavedení postupů** pro hlášení, vyšetřování a nápravu incidentů
- **Role a odpovědnosti** při řešení incidentů
- **Vazba na krizový plán a obnovu provozu** (BCM)

1.7 Model spolupráce a nastavení rozhraní

Zhotovitel musí navrhnout a zajistit model spolupráce s dalšími týmy a případnými třetími stranami:

- **SOC/SIEM tým** – monitorování bezpečnostních událostí
- **Tým záloh a log managementu** – zajištění auditovatelnosti a obnovy
- **Tým krizového řízení nebo BCM** – koordinace přIlncidentech a kontinuitě provozu
- **IT/OT provoz** – technická správa a implementace bezpečnostních opatření

1.8 Školení a povědomí

- **Školení zaměstnanců** o bezpečnostních rizicích, zásadách a postupech
- **Zajištění pravidelného (minimálně ročního) bezpečnostního školení zaměstnanců** ve formě e-learningu nebo prezenčního školení, včetně testování znalostí. Zhotovitel dodá školící materiály a provede první kolo školení.
- **Školení odpovědných osob** po vytvoření metodik a dokumentace

1.9 Reportování a komunikace s vedením organizace

- **Nastavení periodického hlášení** o stavu bezpečnosti
- **Vytvoření pravidelné reportovací zprávy** pro vedení společnosti o:
    - Stavu kybernetické bezpečnosti
    - Incidentech
    - Potřebách pro zajištění rozvoje systému kybernetické bezpečnosti
- **Vytvoření přehledových reportů** vhodných pro management
- **Doporučení pro bezpečnostní KPI:**
    - Počet incidentů a jejich závažnost
    - Auditní zjištění
    - Úspěšnost testování
    - Stav implementace opatření

2. Doplňkové aktivity v roli strategického partnera

Během realizace bude Zhotovitel rovněž:

- **Poskytovat strategické poradenství** v oblasti bezpečnosti

- **Doporučovat preventivní opatření** dle aktuálního vývoje hrozeb
- **Sledovat vývoj legislativy** a upozorňovat na změny dopadající na organizaci
- **Podporovat přípravu na audity**, kontroly nebo simulace incidentů
- **Konzultační činnost** v rozsahu dle požadavků Objednatele

3. Požadavky na přístup k řešení

Řešení musí být přizpůsobeno reálným provozním podmínkám Objednatele, zejména s ohledem na jeho činnost v oblasti správy a provozu rozsáhlého multifunkčního objektu. Veškerá opatření musí být nastavena tak, aby byla:

- **Prakticky proveditelná** – implementovatelná v reálném provozu Objednatele
- **Přenositelná v čase** – s jasnými odpovědnostmi a procesy pro dlouhodobou udržitelnost
- **Auditovatelná** – s odpovídající dokumentací a evidencí
- **Škálovatelná** – schopná reagovat na změny v organizaci a technologiích

Realizace bude rozdělena do několika vzájemně provázaných oblastí, přičemž výstupy budou orientovány na praktickou proveditelnost, přenositelnost a udržitelnost.

4. Požadovaný výsledný stav

Výsledkem spolupráce bude stav, kdy bude Objednatel:

- **Systematicky řídit kybernetická rizika v součinnosti se Zhotovitelem**, včetně odpovědností a procesů
- **Mít zavedenou dokumentaci**, procesy a povědomí odpovědných osob
- **Mít nastavena pravidla** formou bezpečnostních směrnic určujících práva, povinnosti a zásady při práci se systémy
- **Schopen doložit dokumentované postupy a směrnice** v souladu s požadavky regulací
- **Schopen reagovat na incidenty** a eskalovat je správným způsobem
- **Schopen prezentovat svou úroveň bezpečnosti** vedení organizace i externím subjektům (auditorům, dozorovým orgánům)
- **Schopen udržovat a rozvíjet bezpečnostní rámec** vlastními kapacitami nebo za podpory partnera
- **Připraven obstát** v případě kontroly, incidentu nebo externího auditu

4. Služby zajištění kybernetické bezpečnosti za pomoci dohledového centra SOC a provozní monitoring – technická bezpečnostní opatření

Objednatel má zájem o zajištění technických bezpečnostních opatření prostřednictvím služby dohledového centra SOC (Security Operations Center), které bude plnit roli centrálního bodu pro sběr, analýzu a reakci na bezpečnostní události v rámci celé IT a provozní infrastruktury.

Cílem je:

- zajištění včasné detekce anomálií a incidentů napříč síťovými a aplikačními vrstvami,
- vytvoření udržitelného a auditovatelného prostředí pro dohled a kybernetickou bezpečnost,
- nastavení provozně funkčního modelu pro řízení bezpečnostních událostí a eskalací,
- zajištění technické integrace s klíčovými provozními systémy Objednatele.

Postup při nástupu okamžitého řešení s ohledem na charakter incidentu

S ohledem na charakter provozu multifunkční haly ARENA BRNO s vysokou návštěvností veřejných akcí **musí SOC tým Zhotovitele před jakýmkoliv zásahem do infrastruktury (včetně odpojení zařízení nebo vypnutí služeb) vždy nejprve telefonicky konzultovat postup s odpovědnou osobou Objednatele**.

Platí to i v případě závažných bezpečnostních incidentů. Důvodem je, že neplánované odpojení kritických systémů (ticketing, platby, bezpečnostní kamery, wifi apod.), které mohou být napojeny na aktivní prvky dodané Zhotovitelem, během akce s tisíci návštěvníky by mohlo ohrozit bezpečnost osob a způsobit provozní chaos. SOC tým a Objednatel společně najdou kompromisní řešení, které minimalizuje bezpečnostní riziko a současně umožní dokončení probíhající akce, přičemž radikální zásahy budou provedeny až po jejím skončení. Objednatel poskytne SOC týmu Zhotovitele kontaktní seznam odpovědných osob s dostupností 24/7.

Finální řešení pro nástup okamžitého řešení bude zpřesněno v předimplementační analýze, kde Objednatel společně se Zhotovitelem upřesní kritická zařízení i kritické scénáře pro řešení závažných incidentů.

1. Základní komponenty SOC služby a provozního monitoringu

Zhotovitel je povinen navrhnout a realizovat řešení, které zajistí:

1.1 Provoz SOC služby

- **Provoz plně funkčního dohledového centra (SOC)** s garantovanou dostupností a reakčními časy

- **Centralizovaný sběr a správa logů** ze všech relevantních IT a provozních systémů
- **Nasazení vhodných nástrojů** pro:
    - Log management pro sběr a zpracování logů z různých zdrojů
    - Síťovou analýzu s podporou relevantních protokolů (Flow analysis, NDR)
    - Správu bezpečnostních událostí (SIEM/SOAR platforma)
- **SIEM/SOAR platforma** umožňující:
    - Korelaci událostí
    - Behaviorální analýzy
    - Forenzní analýzy
- **Detekční schopnosti** i v rámci izolovaných nebo provozních sítí (např. CCTV, provozní Ethernet, přístupové systémy) – **pokud bude zajištěna TCP/IP konektivita a pokud bude toto umožněno**
- **Přiměřenou automatizaci** reakčních scénářů a reportovacích mechanismů s možností customizace
- **Dlouhodobé uchovávání dat** s možností forenzní analýzy dle požadavků na compliance (minimálně 3 měsíce, doporučeno 18 měsíců)
- **Přehledný bezpečnostní dohled** nad infrastrukturními prvky, servery, aplikacemi a dalšími systémy

1.2 Detekční a analytické schopnosti

- **Detekce pokročilých hrozeb:**
    - Port scanning
    - DoS/DDoS
    - Brute-force útoky
    - Neautorizované přístupy
    - APT (Advanced Persistent Threats)
    - Ransomware aktivity
    - Manipulace s bezpečnostními prvky
    - Aktivity nástrojů pro krádeže identity
- **Behaviorální analýza:** Detekce anomálií na základě historických dat
- **Threat intelligence:** Průběžná aktualizace databází hrozeb a škodlivých indikátorů
- **Korelace událostí:** Napříč všemi zdroji dat pro komplexní pohled na bezpečnost
- **Podpora moderních síťových protokolů** pro analýzu provozu

1.3 Případná Integrace s provozními systémy

Objednatel specifikuje, že řešení pro SOC i provozní monitoring je určeno pouze pro provozní datovou síť a WiFi síť ARENA BRNO, dle kapitol 7 a 8 této přílohy.

Zhotovitel je oprávněn navrhnout řešení pro případné napojení a korelaci s ostatními s provozními systémy, pokud bude zajištěna TCP/IP konektivita a bude v budoucnu bezpečné tyto systémy monitorovat zejména:

- **Systém elektronické kontroly vstupu (EKV)** – za účelem sledování bezpečnostních událostí v návaznosti na fyzický pohyb osob v areálu
- **Docházkový systém** – s cílem analyzovat časové a provozní souvislosti ve vztahu k aktivitám zaznamenaným v síti
- **CCTV systémy** – pokud bude zajištěna TCP/IP konektivita
- **AV Síť** – pokud bude zajištěna TCP/IP konektivita

Tato případná napojení mohou být ze strany Objednatele objednána jako Služby rozvoje.

1.4 Doplňkové bezpečnostní komponenty

- **Ochrana koncových bodů (Endpoint Protection):**
  - Nasazení EDR řešení pro ochranu pracovních stanic a serverů
  - Integrace s centrálním SOC/SIEM systémem
  - Pokrytí všech relevantních koncových zařízení
- **Skenování zranitelností:**
  - Pravidelné autorizované i neautorizované skeny zranitelností
  - Integrace výsledků do SIEM asset databáze
  - Hodnocení závažnosti nálezů
  - Doporučená frekvence: týdenní cyklus
- **Provozní monitoring (Network Monitoring):**
  - Sledování klíčových systémových údajů a dostupnosti prvků IT infrastruktury
  - Notifikace správců při provozních problémech
  - Možnost integrace s SOC pro korelaci provozních a bezpečnostních událostí

1.5 Provozní monitoring

Zhotovitel musí navrhnout a realizovat řešení pro sledování klíčových systémových údajů a dostupnosti prvků v rámci provozní datové sítě a WiFi sítě ARENA BRNO, a to zejména:

- **Provozní monitoring (Network Monitoring):**
  - Sledování klíčových systémových údajů a dostupnosti prvků IT infrastruktury
  - Notifikace správců při provozních problémech
  - Možnost integrace s SOC pro korelaci provozních a bezpečnostních událostí

Pro provozní monitoring je požadováno, aby stavové informace a notifikace byly podpořeny i v českém jazyce, z důvodu, že tyto informace mohou chodit na řízené pracoviště ARENY BRNO (velín), kde obsluha musí okamžitě reagovat a upozornit IT tým. Tyto požadavky vychází nejen

ze zkušenosti samotného provozu, ale i z parametrů nejpoužívanějších open source nástrojů, které se pro provozní mentoring používají, a jsou do českého jazyka lokalizovány.

2. Provozní parametry

2.1 Dostupnost služby

Zhotovitel musí zajistit úrovně SLA dle Přílohy č. 5 Smlouvy.

2.2 Definice priorit bezpečnostních incidentů

Priorita a kategorizace incidentů budou prováděny zejména v souladu se zákonem č. 205/2017 Sb., o kybernetické bezpečnosti (dále jen „ZoKB“), a vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních a kybernetických bezpečnostních incidentech, případně podle klasifikace služby kybernetické bezpečnosti zajišťované prostřednictvím dohledového centra SOC, dle klasifikačních pravidel příslušného SOC centra Zhotovitele. Charakter, závažnost a příklady incidentů však musí být s ohledem na povahu věci zachovány:

Kategorie incidentů:

Kategorie	Popis	Příklady
Závažný incident	Má dopad na poskytování klíčové služby, veřejnost nebo bezpečnost celé organizace	Ransomware útok, masivní data breach, kompromitace kritických systémů, DDoS útok znemožňující provoz, únik citlivých osobních údajů
Střední incident	Ovlivňuje činnost části organizace, může se rozšířit	Malware na více stanicích, phishing kampaň, neoprávněný přístup k necitlivým datům, podezřelá síťová aktivita, lokalizovaný výpadek
Nízký incident	Malý dopad, lokalizovaný problém bez přerušení služeb	Izolovaný malware na jedné stanici, neúspěšný pokus o útok, spam, podezřelý email

Příklady dohledovaných aktiv s možností definice kritičnosti: - Jednotlivé systémy a aplikace - Data (respektive úložiště) - Identity (např. konkrétní privilegované účty)

2.3 Klasifikace řešených incidentů

Vyřešený incident bude klasifikován dle vzorové klasifikace, případně podle klasifikace služby kybernetické bezpečnosti zajišťované prostřednictvím dohledového centra SOC dle klasifikačních pravidel příslušného SOC centra Zhotovitele. Charakter, závažnost a příklady incidentů však musí být s ohledem na povahu věci zachovány:

- **True Positive – KBI**
    - Událost byla vytvořena správně a jedná se o KBI
- **True Positive – Non-Issue**
    - Událost byla vytvořena správně, ale nejedná se o KBI, nebo o případ, kdy je potřeba Událost interně řešit.
- **True Positive – Policy Violation**
    - Událost byla vytvořena správně, nejedná se o KBI, ale je potřeba interně řešit.
- **False Positive – Tuned**
    - Událost není relevantní, chybné vyhodnocení, je nutná úprava pravidla.
- **Ignored**
    - Objednatel (protistrana) nereaguje, nebo nebyla poskytnuta součinnost více než X dní
- **Rule Test**
    - Událost vznikla jako důsledek testování nového Use Case.
- **Undetermined**
    - pro případy, kdy klasifikace není možná ani po analýze.

Za falešně pozitivní incidenty jsou považovány ty, které byly indikovány chybnou logikou detekčního pravidla či chybnými auditními záznamy. Za falešně pozitivní incidenty naopak nejsou považovány ty, které jsou detekovány správně, byla identifikována jejich příčina, ale neznamenají pro organizaci bezpečnostní riziko (např. anomálie v běžném provozu).

2.4 Kapacita řešení incidentů

- **Maximální počet zpracovaných skutečně pozitivních bezpečnostních incidentů za měsíc** (očištěno o falešně pozitivní incidenty) je stanoven dle přílohy č. 5 Smlouvy na 200 Incidentů měsíčně:
    - Závažný incident
        - neomezeně
    - Střední incident
        - Počet v paušálu: 50
    - Nízký incident
        - Počet v paušálu: 150
    - SLA limit stanovuje maximální počet skutečně pozitivních bezpečnostních incidentů, které je Zhotovitel schopen měsíčně řešit. Falešně pozitivní incidenty a provozní anomálie jsou z tohoto limitu vyňaty, jelikož nepředstavují

bezpečnostní riziko a jejich objem nemá přímou vazbu na kvalitu poskytované bezpečnostní služby.

- Incidenty nad rámec uvedeného paušálu budou Objednateli účtovány na základě jednotkové ceny za incident uvedené ve Smlouvě.

2.6 Typ řešení incidentů a typ výstupů při šetření incidentů

Úrovně výstupů:

1. **Úroveň 1 (součást SOC):** Krizový postup pro zamezení šíření – okamžitá reakce (izolace, odpojení, blokace).
2. **Úroveň 2-3 (podpora/konzultace):** Návrh systematického řešení a asistence při implementaci – poskytováno jako podpora nebo v rámci konzultací.
3. **Úroveň 4 (rozvojová činnost):** Vlastní implementace opatření – pouze pokud Zhotovitel spravuje dané prostředí, jinak mimo rozsah SOC.

V rámci SOC musí být zajištěna minimálně úroveň 1 a dále Objednatel upřesňuje, že v případě, že Zhotovitel zároveň spravuje dotčené systémy jím dodané (firewall, servery apod.), je Zhotovitele povinen zajistit i úroveň 2-3 a 4 — tedy vlastní implementaci opatření přímo ve spravovaném prostředí. Tato úroveň reakce je logickým důsledkem správy infrastruktury, kdy Zhotovitel má přímý přístup k jím dodaným systémům, a proto je schopen incident nejen detekovat a izolovat, ale i vyřešit na základě scénářů vyplývajících z předimplementační analýzy nebo po dohodě s Objednatelem.

2.7 Reporting a komunikace

- **Manažerský reporting:**
- **Zasílán e-mailem a slouží i jako podklad pro technickou schůzku**
  - Zasíláno minimálně 1× měsíčně
    - Přehled plnění SLA
    - Přehled zpracovaných incidentů
  - Možnost navýšení frekvence (1× týdně) v rámci rozvojových prací
- **Technické schůzky:**
  - Účast minimálně 1× měsíčně
  - Zaměření na:
    - Optimalizaci detekčních mechanismů
    - Údržbu a rozvoj detekčních pravidel
    - Návrh nových automatizačních scénářů
    - Připojení nových datových zdrojů
    - Tvorbu nových dashboardů
    - Řešení specifických bezpečnostních výzev

- Možnost navýšení frekvence (2× měsíčně)

2.8 Rozvojové práce

Hodinový rozsah zahrnutý v ceně služby – 4h/měsíc

Rozvojové práce zahrnují:

- Úprava a tvorba nových detekčních pravidel a scénářů
- Připojení nových zdrojů
- Optimalizace SIEM nástroje

2.9 Technická podpora

- **Dostupnost:** Hotline a ticket systém nepřetržitě (24×7)
- **Incident Response:** Reakce na bezpečnostní incident
- **Eskalace:** Koordinace s Objednatelem v případě hlášení směrem k národním autoritám (CSIRT.CZ, NÚKIB) při závažných incidentech
- **Technický report:** V případě vážné hrozby obsahující popis incidentu, dopad na organizaci, přijatá opatření a doporučení pro budoucí prevenci

3. Technické komponenty řešení

3.1 Hardwarové zajištění

Zhotovitel musí zajistit:

- **Sběr síťových toků, např.:**
  - Vhodná zařízení pro monitorování síťového provozu
  - Síťové sondy/kolektory pro zpracování síťových dat (Flow)
  - NDR (Network Detection and Response) řešení
- **Centrální komponenty, např.:**
  - Log kolektory nebo relay zařízení pro centralizaci logů
  - SIEM servery (fyzické nebo virtuální)
- **Návrh fyzického rozmístění** sledovacích bodů dle topologie sítě

3.2 Softwarové nástroje

- **SIEM/SOAR platforma:**
  - Korelace bezpečnostních událostí
  - Automatizace reakcí (playbooks)
  - Integrace s threat intelligence
  - Možnost konfigurace vlastních pravidel
  - Podpora standardních formátů a protokolů

- **Log management:**
  - Sběr a zpracování logů z různých zdrojů (syslog, API, agenti, konektory)
  - Normalizace dat
  - Dlouhodobá archivace (minimálně 3 měsíce, doporučeno 18 měsíců)
  - Retenční politika
- **Analýza síťového provozu:**
  - Podpora Flow analýzy
  - NDR schopnosti
  - Detekce anomálií v síťovém provozu
- **Webové GUI (portál, dashboard):**
  - Konfigurovatelné dashboardy
  - Přehled incidentů a alertů
  - Reporting a export funkcionalita (standardní formáty - CSV, PDF, JSON apod.)
  - RBAC (Role-Based Access Control)

3.3 Komunikační nástroje a kanály

Zhotovitel musí navrhnout a realizovat komunikační model zahrnující:

- **SIEM nástroj** (nativní notifikační a incident response systém)
- **Ticketovací systém** Zhotovitele
- **Komunikační platformy** pro běžnou komunikaci
- **Vytvoření komunikační matice** v rámci implementační fáze – definice odpovědných osob, eskalačních cest a komunikačních nástrojů pro každodenní i krizovou komunikaci

3.4 Návrh architektury SOC řešení

Zhotovitel musí v rámci předimplementační analýzy předložit detailní návrh architektury (a zvolené řešení následně realizovat), který bude zahrnovat:

3.4.1Návrh architektury

Grafické znázornění zahrnující:

- **Centrální roli SIEM platformy** jako orchestrátora bezpečnostních událostí
- **Napojení na zdrojové systémy:**
  - Active Directory
  - Servery (Windows, Linux)
  - Síťové prvky (směrovače, přepínače, firewally)
  - Aplikace a databáze
- **Případné návrh zapojení na provozní systémy nebo další datové sítě, pokud bude zajištěna TCP/IP konektivita a bude to možné z pohledu bezpečnosti**

    - **Objednatel specifikuje, že řešení pro SOC i provozní monitoring je určeno pouze pro provozní datovou síť a WiFi síť ARENA BRNO, dle kapitol 7 a 8 této přílohy.**
    - Zhotovitel je oprávněn navrhnout rozšíření pro případné napojení a korelaci s ostatními s provozními systémy, pokud bude zajištěna TCP/IP konektivita a bude v budoucnu bezpečné tyto systémy monitorovat zejména:
        - **Systém elektronické kontroly vstupu (EKV)** – za účelem sledování bezpečnostních událostí v návaznosti na fyzický pohyb osob v areálu
        - **Docházkový systém** – s cílem analyzovat časové a provozní souvislosti ve vztahu k aktivitám zaznamenaným v síti
        - **CCTV systémy** – pokud bude zajištěna TCP/IP konektivita
        - **AV Síť** – pokud bude zajištěna TCP/IP konektivita
- **Tok dat mezi komponentami:**
    - Směr toku dat (sběr logů, síťový provoz, notifikace, reporty)
    - Bod sběru síťového provozu (např. core switch)
    - Umístění sond a kolektorů
- **Bezpečnostní vrstvy:**
    - Auditní logy
    - Segmentace přístupů
    - Autentizace a autorizace

3.4.2 Popis umístění komponent

Zhotovitel v rámci předimplementační analýzy specifikuje, kde budou jednotlivé komponenty umístěny:

- **Centrální datacenter (DC):**
    - SIEM server (fyzický nebo virtuální)
    - Funkce: Log management + SIEM + retenční databáze
    - Specifikace retence dat (např. 18 měsíců)
- **Síťové sondy a kolektory:**
    - Umístění síťových sond pro odposlech síťového provozu
    - Funkce: Sběr dat o síťovém provozu (Flow), generování Flow ze zachyceného provozu
    - Zhotovitel musí uvést, z kolika míst bude prováděn odposlech (např. jeden centrální bod na core switch pro sledování příchozího/odchozího provozu)
- **Skenery zranitelností:**
    - Umístění skeneru (fyzický server nebo virtuální appliance)
    - Funkce: Autorizované a neautorizované skeny zranitelností
    - Viditelnost: Musí mít TCP/IP konektivitu na všechny skenované systémy a porty
    - Zhotovitel musí uvést, z kolika míst bude prováděno skenování

- **Provozní monitoring:**
    - Umístění monitorovacího serveru (fyzický nebo virtuální appliance)
    - Funkce: Sledování klíčových systémových údajů, dostupnosti prvků IT infrastruktury
    - Způsob sběru dat: Agenti, remote sondy
    - Notifikace: Přímé zasílání na správce (mimo SOC)

3.4.3 Popis funkce jednotlivých komponent

Základní funkce systému:

1. **Konfigurace logování:**
    - Na všech klíčových prvcích infrastruktury se zkonfiguruje logování
    - Konektory SIEM provádějí sběr logů nebo příjem přes syslog
    - Uložení logů v souladu s retenční politikou
    - Sběr probíhá v definovaných intervalech (např. několikaminutových)
2. **Normalizace a uložení:**
    - Sesbírané logy jsou normalizovány
    - Uložení v retenční databázi
3. **Sběr síťového provozu:**
    - Paralelní sběr Flow nebo generování Flow ze zachyceného síťového provozu
4. **Skenování zranitelností:**
    - Pravidelné autorizované a neautorizované skeny (týdenní cyklus)
    - Výsledky skenů přenášeny do SIEM asset databáze
    - Využití pro hodnocení závažnosti nálezů SIEM
5. **Zpracování událostí:**
    - Báze pravidel v SIEM systému generuje bezpečnostní události
    - Události zpracovává služba SOC v nabízeném SLA
6. **Provozní monitoring:**
    - Samostatný systém pro sledování systémových údajů a dostupnosti
    - Zasílání notifikací přímo na správce technologických celků
    - **Důležité:** Reakce na provozní problémy není součástí SOC služby (Zhotovitel musí specifikovat, jak bude řešena)

3.4.4 Dopady výpadku komponent

Zhotovitel musí v rámci předimplementační analýzy specifikovat:

- **Co se stane při výpadku SIEM serveru:**
    - Zda bude pokračovat sběr síťového provozu
    - Zda bude fungovat dočasné ukládání dat
    - Jak dlouho může být systém nefunkční bez ztráty dat
- **Co se stane při výpadku síťové sondy:**

    - Zda bude pokračovat sběr logů
    - Jaká data budou ztracena
- **Zda jsou komponenty distribuované:**
    - Redundance kritických komponent
    - Možnost záložního provozu

3.5 Licenční model

Zhotovitel v rámci předimplementační analýzy předloží návrh licencování produktů s ohledem na:

- **Typ licenčního modelu:**
    - Perpetual vs. Subscription
    - Licencování dle počtu zdrojů, EPS (Events Per Second), uživatelů nebo jiné metriky
- **Rozsah aktualizací a údržby:**
    - Maintenance poplatky
    - Frekvence aktualizací
    - Podpora nových verzí
- **Dopady při přerušení licenčního vztahu:**
    - Funkčnost systému po ukončení licence
    - Možnost exportu dat
    - Migrace na jiné řešení
- **Funkční omezení:**
    - Co přestane fungovat při ukončení platnosti licencí
    - Dopady na archivovaná data
    - Dopady na přístup k historickým datům

4. Implementační fáze

Zhotovitel musí zajistit komplexní implementaci v následujících krocích:

4.1 Analýza a návrh

V rámci předimplementační analýzy Zhotovitel provede:

- **Analýzu současného stavu** IT a provozní infrastruktury Objednatele
- **Návrh optimalizace** z pohledu bezpečnostního dohledu a auditovatelnosti
- **Identifikaci napojovaných zdrojů** a způsobu sběru dat
- **Návrh topologie** z pohledu viditelnosti a bezpečnostního dohledu
- **Posouzení dopadů** na provozní dostupnost a auditní požadavky

4.2 Dodávka a instalace

- **Dodávka všech hardwarových komponent** dle specifikace
- **Instalace softwarových nástrojů** (SIEM, log management, NDR, skenery)
- **Instalace integračních prvků** (konektory, agenti, kolektory)

4.3 Konfigurace a integrace

- **Konfigurace SIEM platformy:**
  - Založení a základní konfigurace
  - Návrh strategie ukládání dat (Analytics vs. archivní úložiště)
  - Instalace detekčních balíčků a šablon
  - Aktivace a konfigurace retenční politiky
- **Napojení datových konektorů** (initial onboarding)
- **Vytvoření RBAC skupin** pro SOC tým a další oprávněné osoby
- **Konfigurace automatizací:**
  - Vytvoření a nahrání seznamů sledovaných entit (watchlists)
  - Implementace automatizačních scénářů (playbooks)
  - Integrace s AI/ML nástroji (pokud podporováno)
- **Tvorba a implementace detekčního obsahu:**
  - Definice detekčních scénářů a pravidel
  - Nastavení priorit a eskalačních cest
  - Optimalizace pro minimalizaci falešně pozitivních hlášení
- **Nastavení dlouhodobé retence** pro veškeré datové zdroje

4.4 Napojení dalších systémů

- **Objednatel specifikuje, že řešení pro SOC i provozní monitoring je určeno pouze pro provozní datovou síť a WiFi síť ARENA BRNO, dle kapitol 7 a 8 této přílohy.**
- Zhotovitel je oprávněn navrhnout rozšíření pro případné napojení a korelaci s ostatními s provozními systémy, pokud bude zajištěna TCP/IP konektivita a bude v budoucnu bezpečné tyto systémy monitorovat zejména:
  - **Systém elektronické kontroly vstupu (EKV)** – za účelem sledování bezpečnostních událostí v návaznosti na fyzický pohyb osob v areálu
  - **Docházkový systém** – s cílem analyzovat časové a provozní souvislosti ve vztahu k aktivitám zaznamenaným v síti
  - **CCTV systémy** – pokud bude zajištěna TCP/IP konektivita
  - **AV Síť** – pokud bude zajištěna TCP/IP konektivita

4.5 Testování a optimalizace

- **Testování detekčních schopností** s cílem minimalizovat falešně pozitivní hlášení
- **Ověření funkčnosti** všech integračních bodů

- **Optimalizace výkonu** a reakčních časů

4.6 Školení a předání

- **Školení personálu Objednatele** pro práci s dohledovým systémem a reporty
- **Školení administrátorů** pro správu a údržbu systému
- **Předání provozní dokumentace:**
  - Technická dokumentace systému a konfigurace
  - Provozní příručky pro administrátory
  - Uživatelské manuály pro operátory velína
    - dokumentace je určena a zamýšlena pro obsluhu velínu, která může být z personálních důvodů prvním přijímajícím kontaktem notifikaci například o probíhajícím bezpečnostním incidentu nebo útoku. Obsluha musí mít k dispozici srozumitelný postup v českém jazyce, jak danou situaci vyhodnotit a dle eskalační matice kontaktovat IT tým nebo Security tým. Manuál je proto nezbytnou součástí provozní dokumentace.
  - Postupy pro incident response a eskalaci
  - Disaster recovery plán pro SOC služby

4.7 Zahájení provozu

- **Zahájení 24/7 provozu SOC služby** s garantovanými SLA parametry
- **Plná technická podpora** od okamžiku zahájení provozu

5. Údržba a rozvoj

Kontinuální služby zahrnující:

5.1 Pravidelná údržba

- **Pravidelná profylaxe** a kontrola konfigurace všech SOC komponent
- **Change management** dle best-practice postupů
- **Aktualizace verzí** v rámci řízeného procesu změn
- **Monitoring zdraví systému** (kapacita úložiště, výkon CPU, paměť, dostupnost služeb)

5.2 Měsíční reporting

- **Stav systému** (dostupnost, výkon, kapacita)
- **Detekované události** a zpracované incidenty
- **Statistiky** (počet incidentů dle priorit, typy hrozeb, trendy)
- **Doporučení** pro zlepšení bezpečnosti

5.3 Konzultační podpora

- **Analytická podpora** při implementaci nových komponent

- **Podpora při budoucím rozvoji** infrastruktury
- **Reakce na aktuální bezpečnostní hrozby** a jejich dopady
- **Doporučení preventivních opatření** dle aktuálního vývoje hrozeb

6. Vymezení rozsahu dodávky

6.1 Co je součástí dodávky

- Základní komponenty SOC služby
- Hardwarové a softwarové komponenty
- Implementace a onboarding
- Školení personálu
- Provozní dokumentace
- 24/7 SOC služba s definovaným SLA dle přílohy č. 5 Smlouvy

6.2 Požadavky na součinnost Objednatele

- Zajištění přístupů k systémům a infrastruktuře
- Nominování odpovědných osob pro komunikaci (technické kontakty, manažerské kontakty)
- Účast na implementačních aktivitách (onboarding, testování)
- Poskytnutí informací o infrastruktuře a síťové topologii
- Zajištění potřebných technických účtů a oprávnění pro integraci systémů

6.3 Model post-implementační podpory

- **Servisní podpora:**
  - dle přílohy č. 5 Smlouvy
- **Konzultační služby** v rozsahu Služeb podpory
- **Rozvojové práce** dle Smlouvy
- **Školení a know-how transfer** (frekvence, rozsah dle Smlouvy)

7. Charakteristika prostředí a kompatibilita

Řešení musí odpovídat charakteru prostředí **multifunkční haly** a umožnit koordinovanou správu technických bezpečnostních opatření. Systém musí být plně kompatibilní s dalšími bezpečnostními systémy organizace, včetně plánů BCM, DRP a IRP.

Důraz je kladen na:

- **Auditovatelnost** všech procesů a událostí
- **Rozšiřitelnost** pro budoucí potřeby Objednatele
- **Technickou udržitelnost** a dlouhodobou podporu řešení
- **Minimalizaci dopadů** na běžný provoz během implementace

- **Soulad s legislativou** (Zákon č. 264/2025 Sb., o kybernetické bezpečnosti, GDPR, NIS2)
- **Škálovatelnost** řešení při růstu infrastruktury
- **Podpora českého jazyka** v uživatelském rozhraní a dokumentaci
- **Místní technická podpora** pro rychlou reakci na incidenty
- **Schopnost koordinace** s národními bezpečnostními autoritami (CSIRT.CZ, NÚKIB)

8. Požadované výstupy od Zhotovitele

8.1 Projektová dokumentace

- **Detailní návrh architektury** SOC řešení s odůvodněním volby technologií, včetně popisu architektury dle sekce 3.4
- **Implementační plán** s časovým harmonogramem
- **Specifikace všech komponent** včetně technických parametrů (CPU, RAM, HDD, síťové porty, redundance)
- **Cenová kalkulace** s rozpisem nákladů na:
    - Jednotlivé hardwarové komponenty
    - Softwarové licence
    - Implementační projekt
    - Měsíční provozní náklady SOC služby

8.2 Provozní dokumentace

- Technická dokumentace systému a konfigurace
- Provozní příručky pro administrátory
- Uživatelské manuály pro operátory
- Postupy pro incident response a eskalaci
- Disaster recovery plán pro SOC služby

8.3 Záruky a SLA

- **SLA** dle přílohy č. 5 Smlouvy
- **Záruční podmínky** na všechny dodané komponenty (dle Smlouvy)
- **Postupy pro řešení poruch** a výpadků
- **Plán kontinuity služeb** při kritických situacích

5. Služby zálohování a archivace ICT dat – technická specifikace

Objednatel má zájem o návrh a implementaci řešení pro zálohování a archivaci dat, které bude tvořit integrální součást celkové ICT infrastruktury společnosti ARENA BRNO, a.s. Cílem je zavedení centralizovaného systému zálohování a dlouhodobé archivace, který zajistí bezpečnost, obnovitelnost a provozní kontinuitu v souladu s platnou legislativou a v návaznosti na plánovanou virtualizační a serverovou platformu.

Archivací se myslí z pohledu Objednatele dlouhodobá záloha.

Cílem je:

- zajištění bezpečného, pravidelného a auditovatelného zálohování systémových, aplikačních a provozních dat,
- vytvoření udržitelného prostředí pro dlouhodobou archivaci, ve smyslu dlouhodobé zálohy
- posílení odolnosti vůči výpadkům, chybám i kybernetickým hrozbám,
- sjednocení správy záloh a archivace v rámci jednotného infrastrukturního konceptu,
- podpora plánovaných scénářů obnovy včetně replikace záloh do oddělené lokality.

1. Základní požadavky na řešení

1.1 Rozsah zálohování

Zhotovitel je povinen navrhnout a realizovat řešení, které zajistí zálohování:

- **Virtualizovaných prostředí:**
  - Virtualizační platforma dodaná Zhotovitelem
  - Virtuální servery a aplikace
- **Fyzických serverů:**
  - Fyzické servery včetně aplikačních a databázových služeb, které jsou součástí dodávky Zhotovitele
- **Koncových stanic:**
  - Pracovní stanice dle potřeby, pokud budou součástí dodávky Zhotovitele.
  - Objednatel počítá s tím, že archivace pracovních stanic (např. z prostředí pokladen, gastronomických systémů a dalších) bude realizována v počtu a rozsahu dle nabídky Zhotovitele a dodávky v rámci rozvojových prací, z důvodu, že v současné době není znám jejich přesný rozsah ani počet.
  - Objednatel informuje Zhotovitele, že dodané řešení musí být škálovatelné pro tyto budoucí potřeby.
- **Cloudových služeb:**

    - Cloudové služby (Microsoft 365, a to konkrétně: Exchange OnLine, SharePoint OnLine, OneDrive, případně Teams.)
- **Aplikačních záloh:**
    - Databáze a aplikační data dle dodaného zálohovacího nástroje Zhotovitele

1.2 Archivace dat

Zhotovitel musí navrhnout a realizovat řešení pro dlouhodobou archivaci vybraných datových oblastí:

- E-mailová komunikace
- Účetní doklady
- Personální dokumentace
- Soubory logů (například z IDM, RadiusServeru a jiných)
- Další data dle požadavků legislativy

2. Parametry prostředí a kapacitní požadavky

2.1 Charakteristika prostředí

Objednatel požaduje využití:

- **Dvojice centrálních datacenter (DC)** propojených vysokorychlostní sítí
- **Primární DC (DC1):**
    - Virtualizační servery (např. dvojice Hyper-V serverů nebo ekvivalent)
    - Produkční diskové pole s kapacitou minimálně 30 TB
    - Několik fyzických serverů, dle návrhu Zhotovitele
- **Sekundární DC (DC2):**
    - Paralelní infrastruktura pro účely DR a offsite replikace pro kritické služby

2.2 Kapacitní parametry

Zhotovitel musí navrhnout řešení pro následující kapacity:

- **Celkový počet zálohovacích úloh (workloads):** 50
- **Objem zálohovaných dat:** 20-35 TB
- **Počet uživatelů cloudových služeb (O365):** 50
- **Očekávaná deduplikace:** cca 50 % (Zhotovitel uvede reálné hodnoty pro navržené a realizované řešení nebo hodnoty deklarované výrobcem)
- **Očekávaná komprese:** cca 30 % (Zhotovitel uvede reálné hodnoty pro navržené a realizované řešení nebo hodnoty deklarované výrobcem)
- **Očekávaná celková kapacita úložiště záloh:** min. 100 TB – Zhotovitel vypočítá podle vlastního návrhu)

3. Technické požadavky na řešení

3.1 Vlastnosti zálohovacího systému

Zhotovitel musí navrhnout řešení, které zajistí:

- **Centralizovanou správu:**
  - Jednotný nástroj pro správu všech zálohovacích úloh
  - Webové GUI nebo tlustý klient pro správu
  - Centrální reporting a monitoring
- **Integraci s virtualizační platformou:**
  - Minimalizace dopadů zálohovacích procesů na provozované prostředí
  - Podpora snapshotů na úrovni hypervisoru
- **Verzování a retenci záloh:**
  - Možnost uchovávání více verzí zálohovacích bodů
  - Konfigurovatelné retenční politiky
- **Ochranné mechanismy:**
  - WORM / imutabilní režim ukládání záloh
  - Ochrana proti ransomware
  - Šifrování záloh (doporučeno AES-256 nebo ekvivalent)
- **Právní blokace (Legal Hold):**
  - Nezávislé uchovávání kopií mimo standardní retenční politiku např. aplikačně či procesně formou:
    - oddělené zálohy
    - prodloužená retence
    - omezený přístup
    - auditní logy
- **Replikaci a offsite zálohování:**
  - Možnost replikace záloh do sekundárního DC
  - Podpora offsite archivace (např. páskové médium)

3.2 Zálohovací schéma a retenční politika

Zhotovitel navrhne zálohovací schéma odpovídající potřebám Objednatele. **Orientační schéma** (Zhotovitel může navrhnout vlastní):

Typ zálohy	Frekvence	Retence	Úložiště / Poznámka
Denní inkrementální	1× denně	7-30 dní	Primární DC1 (diskové, rychlé)
Synthetic full (týdenní)	1× týdně	4 týdny	Primární DC1
Měsíční plná záloha	1× měsíčně	12 měsíců	Sekundární DC2 (imutabilní)
Roční plná záloha	1× ročně	5-10 let	Archivace na pásky (volitelné)

Zhotovitel v rámci předimplementační analýzy specifikuje: - Typ záloh (full, incremental, differential, synthetic full) - Frekvenci a časové okno pro provádění záloh - Retenční politiku pro jednotlivé typy záloh - Schéma GFS (Grandfather-Father-Son) nebo ekvivalent

3.3 Kapacitní plán

Zhotovitel v rámci předimplementační analýzy předloží kapacitní plán pro navržené řešení zahrnující:

- **Vstupní parametry:**
  - Objem zálohovaných dat (GB/TB)
  - Očekávaná deduplikace (%)
  - Očekávaná komprese (%)
  - Efektivní velikost zálohy
- **Výpočet kapacity úložiště:**
  - Kapacita pro denní zálohy
  - Kapacita pro týdenní zálohy
  - Kapacita pro měsíční zálohy
  - Kapacita pro roční zálohy
  - **Celková požadovaná kapacita úložiště**

Příklad kapacitního plánu (Zhotovitel vypočítá podle vlastního návrhu):

Typ zálohy	Počet záloh	Jednotková velikost	Celková velikost
Denní	7-30	X TB	Y TB
Týdenní	4	X TB	Y TB
Měsíční	12	X TB	Y TB
Roční	5-10	X TB	Y TB
CELKEM			**Z TB**

4. Architektura řešení

4.1 Komponenty zálohovacího systému

Zhotovitel musí navrhnout a realizovat architekturu zahrnující:

4.1.1 Zálohovací server (Backup Server)

- **Umístění:** Primární DC (DC1) nebo virtuální instance
- **Funkce:**
  - Centrální správa konfigurace
  - Scheduling zálohovacích úloh
  - Backup proxy (volitelně)
  - Management rozhraní (webové GUI nebo tlustý klient)
- **Technické parametry** (Zhotovitel specifikuje):
  - CPU (počet jader, frekvence)
  - RAM (kapacita v GB)
  - HDD (kapacita v GB/TB)
  - OS (Windows Server, Linux nebo ekvivalent)
  - Fyzický server nebo virtuální instance

4.1.2 Zálohovací úložiště (Backup Repository)

Zhotovitel navrhne a realizuje úložiště záloh s následujícími vlastnostmi:

- **Primární úložiště:**
  - Umístění v primárním DC (DC1)
  - Rychlý přístup pro obnovu dat
  - Možnost využití diskového pole nebo dedikovaného serveru
- **Sekundární úložiště (Hardened/Immutable Repository):**
  - Umístění v sekundárním DC (DC2) nebo oddělené lokalitě
  - Ochrana proti ransomware (imutabilní úložiště)
  - Fyzická nebo logická separace od produkční infrastruktury
- **Technické parametry úložiště** (Zhotovitel specifikuje):
  - Typ úložiště (HDD/SSD) s rozhraním (SAS nebo SATA) nebo NAS
  - Kapacita (TB)
  - RAID konfigurace
  - Síťové rozhraní (1GbE nebo 10GbE nebo 25GbE)
    - Pro přenos větších dat preferuje Objednatel rozhraní od 10GbE
  - Redundance (zdroje napájení, síťové karty)

4.1.3 Proxy servery (Backup Proxy)

- **Funkce:**

    - Zpracování zálohovacích úloh
    - Minimalizace zatížení produkční infrastruktury
    - Viditelnost na všechny zdrojové systémy
- **Umístění:**
    - V primárním DC
    - Možnost více proxy serverů pro distribuci zátěže
        - Objednatel navrhuje umístění proxy serverů pouze v DC1, protože primární zálohovací proces bude probíhat nad servery umístěnými v primárním datacentru. Sekundární DC (DC2) bude využito pouze pro offsite replikaci záložních kopií a imutabilní úložiště, kde již proxy servery nejsou potřeba.
- **Technické parametry** (Zhotovitel specifikuje):
    - Počet proxy serverů
    - Umístění (fyzické nebo virtuální)
    - CPU, RAM, HDD

4.1.4 Páskové úložiště (volitelně)

Zhotovitel může navrhnout páskové úložiště pro:

- **Dlouhodobou archivaci:**
    - Offsite archivace pro legislativní požadavky
    - Retence 5-10 let
- **Technické parametry** (pokud navrženo):
    - Typ páskové knihovny (LTO-9 nebo novější)
    - Počet slotů
    - Počet pásek
    - Kapacita na pásku
    - Připojení (SAS nebo FC)

4.1.5 Další komponenty

- **Komponenty pro cloudové zálohování:**
    - Gateway pro zálohování cloudových služeb (např. O365)
    - Technické parametry (CPU, RAM, HDD)
- **Komponenty pro zálohování fyzických serverů:**
    - Agenti pro fyzické servery
    - Proxy servery pro zpracování záloh fyzických serverů

4.2 Diagram architektury

Zhotovitel musí v rámci předimplementační analýzy předložit diagram nebo technický popis architektury zahrnující:

- **Umístění komponent:**
  - Zálohovací server v DC1
  - Primární úložiště v DC1
    - Toto umístění je přípustné, případně záleží na návrhu Zhotovitele dle předloženého schématu provozní datové sítě a jednotlivých IDF/MDF.
  - Sekundární úložiště v DC2
  - Páskové úložiště (pokud navrženo)
  - Proxy servery
- **Tok dat:**
  - Směr zálohovacích operací
  - Replikace mezi DC1 a DC2
  - Archivace na pásky (pokud navrženo)
- **Bezpečnostní vrstvy:**
  - Šifrování
  - RBAC přístupy
  - Auditní logy

4.3 Zálohovací politika

Zhotovitel v rámci předimplementační analýzy navrhne zálohovací politiku zahrnující:

- **Primární zálohování:**
  - Zálohy na primární úložiště v DC1
  - Typ záloh (např. synthetic full + forward incrementals)
  - Frekvence a retence
- **Replikace záloh mezi DC:**
  - Kopírování záloh z DC1 do DC2
  - Typ úlohy (např. Copy Backup Job)
  - Frekvence replikace
- **Archivace na pásky** (pokud navrženo):
  - Výběr dat pro archivaci
  - Frekvence (např. měsíční full backup)
  - Retence (např. 1-10 let)

Příklad schématu:

Typ zálohy	Frekvence	Retence	Úložiště / Poznámka
Denní inkrementální	1× denně	7-30 dní	Primární DC1 (diskové, rychlé)
Synthetic full (týdenní)	1× týdně	4 týdny	Primární DC1
Měsíční plná záloha	1× měsíčně	12 měsíců	Sekundární DC2 (imutabilní)
Roční plná záloha	1× ročně	5-10 let	Archivace na pásky (volitelné)

4.4 Vysoká dostupnost (HA)

Zhotovitel musí v rámci předimplementační analýzy specifikovat:

- **Úroveň HA zálohovacího serveru:**
  - Zda je zálohovací server virtualizovaný s podporou HA na úrovni hypervisoru
  - Nebo zda je fyzický server s redundantními komponentami
- **Dopady výpadku zálohovacího serveru:**
  - Co se stane při výpadku primárního zálohovacího serveru
  - Jak dlouho může být systém nefunkční bez ztráty dat
- **Redundance kritických komponent:**
  - Zálohovací server (virtuální nebo fyzický)
  - Síťové připojení
  - Úložiště

5.1 Architektura archivačního systému

Zhotovitel v rámci předimplementační analýzy navrhne architekturu zahrnující:

5.1.1 Aplikační vrstva

- **Umístění:** Virtuální instance v DC1
- **Funkce:**
  - Management rozhraní (Web GUI, Web API)
  - Integrace s externími systémy
- **Technické parametry** (Zhotovitel specifikuje):
  - CPU (počet jader)
  - RAM (kapacita v GB)
  - HDD (kapacita v GB)
  - OS (Windows Server, Linux nebo ekvivalent)

5.1.2 Databázové úložiště

- **Funkce:** Úložiště strukturovaných dat archivu
- **Umístění:** Dedikovaná databázová instance (sdílená nebo samostatná)
- **Technické parametry** (Zhotovitel specifikuje):
    - Typ databáze (MS SQL, PostgreSQL nebo ekvivalent)
    - Kapacita RAM dedikovaná instanci
    - Kapacita úložiště

5.1.3 Úložiště contentu

- **Funkce:** Ukládání archivovaných souborů
- **Umístění:** Distribuováno mezi DC1 a DC2
- **Technické parametry** (Zhotovitel specifikuje):
    - Počet souborových serverů
    - Kapacita každého serveru (TB)
    - Protokoly (SMB, NFS nebo iSCSI)
    - Redundance a ochrana dat

6. Ochrana zálohovacích a archivačních procesů

6.1 Bezpečnostní opatření

Zhotovitel musí zajistit:

- **Šifrování dat:**
    - Šifrování záloh (doporučeno AES-256 nebo ekvivalent)
    - Šifrování během přenosu (TLS/SSL)
- **Řízení přístupu (RBAC):**
    - Definice rolí a oprávnění
    - Integrace s Active Directory nebo ekvivalentem
- **Auditní záznamy:**
    - Sběr a archivace auditních logů
    - Integrace s centrálním SIEM systémem (pokud existuje)
- **Multifaktorová autentizace (2FA):**
    - Možnost aktivace 2FA pro správu systému

6.2 Ochrana proti ransomware

Zhotovitel musí implementovat:

- **Imutabilní úložiště:**
    - WORM režim v sekundárním DC
    - Ochrana proti neoprávněné manipulaci nebo smazání záloh
- **Detekce ransomware:**

    - Skenovací engine pro detekci výskytu ransomware v zálohovacích úlohách
    - Nebo alternativní mechanismus detekce anomálií
- **Offsite zálohy:**
    - Umístění záloh v sekundárním datovém centru (DC2) odděleném od produkční infrastruktury, a to formou fyzické a/nebo logické separace
    - Pro účely tohoto dokumentu se offsite zálohou rozumí uložení záloh v druhém datovém centru v rámci objektu Objednatele, nikoli mimo geografickou lokalitu

7. Disaster Recovery a obnova dat

7.1 Požadavky na obnovu

Zhotovitel musí navrhnout scénáře obnovy zahrnující:

- **RPO (Recovery Point Objective):**
    - Zhotovitel navrhne dosažitelné RPO pro různé systémy
    - Orientačně: RPO ≤ 24 hodin pro nekritické systémy, RPO ≤ 4 hodiny pro kritické systémy
- **RTO (Recovery Time Objective):**
    - Zhotovitel navrhne dosažitelné RTO pro různé systémy
    - Orientačně: RTO ≤ 4 hodiny pro kritické systémy s objemem dat do cca 2 TB, u větších objemů bude doba obnovy proporcionálně delší; RTO ≤ 24 hodin pro nekritické systémy.

8. Integrace a kompatibilita

8.1 Integrace s existující infrastrukturou

Zhotovitel musí zajistit integraci s:

- **Virtualizační platformou:**
    - Podpora virtualizační platformy dodané Zhotovitelem
    - Integrace snapshotů a API
- **Cloudové služby:**
    - Zálohování Microsoft 365

8.2 Integrace s nástroji pro správu a dohled

Zhotovitel zajistí integraci s:

- **Monitorovací nástroje:**
    - Standardizovaná rozhraní (SNMP, SYSLOG)
    - Specifické pluginy pro monitorování zálohovacího systému
- **SOC (Security Operations Center):**

    - Integrace pro bezpečnostní dohled
    - Notifikace při bezpečnostních událostech

9. Licenční model

9.1 Požadavky na licencování

Zhotovitel v rámci předimplementační analýzy předloží návrh licencování produktů s ohledem na:

- **Typ licenčního modelu:**
    - Perpetual vs. Subscription
    - Licencování dle počtu procesorů, instancí, uživatelů, kapacity nebo jiné metriky
- **Rozsah licence:**
    - Pokrytí všech navržených komponent
    - Možnost budoucího růstu bez dodatečných nákladů (doporučeno)
- **Maintenance a podpora:**
    - Nárok na aktualizace a opravy
    - Frekvence aktualizací
    - Podpora nových verzí
- **Dopady při ukončení licence:**
    - Funkčnost systému po ukončení licence
    - Možnost exportu dat
    - Migrace na jiné řešení

9.2 Přípustné licenční modely

Zhotovitel v rámci svého řešení zvolí jednu z následujících možností licencování:

- Licencování dle procesorů (CPU)
    - Výhody: Neomezený růst počtu virtuálních strojů
    - Nevýhody: Vyšší počáteční náklady
- Licencování dle instancí/workloads (např. Universal License)
    - Výhody: Nižší počáteční náklady
    - Nevýhody: Růst nákladů při rozšiřování infrastruktury
- Licencování dle kapacity dat
    - Výhody: Jednoduché plánování nákladů
    - Nevýhody: Omezení při růstu dat

10. Implementace a předání do provozu

10.1 Fáze implementace

Zhotovitel zajistí komplexní implementaci v následujících krocích:

10.1.1 Kickoff a analýza

- Kickoff meeting
- Analýza p*ro přípravu navazujících implementačních kroků*
- Návrh scénářů obnovy a retenčních pravidel
- Posouzení dopadů na provozní dostupnost, tak aby byl zajištěn provozní monitoring

10.1.2 Dodávka a montáž

- Dodávka všech hardwarových komponent
- Montáž do racků
- Zapojení do sítě

10.1.3 Instalace a konfigurace

- Instalace zálohovacího serveru
- Instalace a konfigurace úložišť (primární, sekundární, pásky)
- Konfigurace proxy serverů

10.1.4 Konfigurace zálohovacích úloh

- Konfigurace zálohování virtuální infrastruktury
- Konfigurace zálohování fyzických serverů
- Konfigurace zálohování cloudových služeb (např. O365)
- Konfigurace zálohování NAS úložišť

10.1.5 Integrace

- Integrace s monitorovacími nástroji
- Integrace s SOC
- Konfigurace auditních záznamů

10.1.6 Testování

- Testování funkčnosti zálohovacích úloh
- Testování obnovy dat
- Testování vysoké dostupnosti (pokud aplikovatelné)
- Testování DR scénářů

10.1.7 Dokumentace a školení

- Zpracování technické dokumentace
- Školení administrátorů
- Předání dokumentace

10.1.8 Akceptace a předání

- Akceptační testy
- Předání do produkčního provozu

10.2 Časový rámec implementace

Zhotovitel v rámci předimplementační analýzy předloží harmonogram implementace s konkrétními milníky a termíny odpovídající výše uvedeným fázím a termínům dle Smlouvy.

11. Vymezení rozsahu dodávky

11.1 Co je součástí dodávky

- Kompletní služba návrhu řešení
- Dodávka a instalace všech HW a SW komponent
- Konfigurace zálohovacího systému
- Konfigurace archivačního systému (pokud součástí)
- Školení administrátorů
- Technická dokumentace
- Konzultační a metodická podpora:
    - Analýza zálohovaných systémů a datových toků
    - Návrh scénářů obnovy a retenčních pravidel
    - Podpora pro Disaster Recovery plánování
- Provozní podpora dle SLA

11.2 Požadavky na součinnost Objednatele

- Zajištění přístupů k systémům a infrastruktuře
- Nominování odpovědných osob
- Účast na implementačních aktivitách
- Poskytnutí informací o infrastruktuře

12. Požadované výstupy od Zhotovitele

12.1 Projektová dokumentace

- **Detailní návrh architektury** zálohovacího a archivačního řešení s odůvodněním volby technologií
- **Diagram architektury** (umístění komponent, tok dat, bezpečnostní vrstvy)
- **Kapacitní plán** s výpočtem požadované kapacity úložiště
- **Implementační plán** s časovým harmonogramem a milníky
- **Specifikace všech komponent** včetně technických parametrů (CPU, RAM, HDD, síťové rozhraní, redundance)

12.2 Provozní dokumentace

- Technická dokumentace systému a konfigurace
- Zálohovací plány a retenční politiky
- Provozní příručky pro administrátory
- Postupy pro obnovu dat
- Disaster Recovery plán
- Dokumentace testů obnovitelnosti
- Známé postupy pro řešení poruch a výpadků

12.3 SLA a záruky

- SLA dle přílohy č. 5 Smlouvy
- Záruční podmínky na všechny dodané komponenty dle Smlouvy

6. Služby virtualizace a serverové infrastruktury – technická specifikace

Objednatel má zájem o implementaci a provoz virtualizované serverové infrastruktury, která bude sloužit jako základní provozní prostředí pro běh aplikačních a systémových služeb společnosti ARENA BRNO, a.s. Řešení musí zahrnovat vysokodostupnou virtualizační platformu (na úrovni technických možností jednoho clusteru se dvěma servery, jak je požadováno Objednatelem), centrální úložný systém a komplexní správu virtualizovaného prostředí s důrazem na spolehlivost a škálovatelnost.

Cílem je:

- zajištění stabilní a vysoce dostupné virtualizační infrastruktury pro kritické systémy Objednatele,
- vytvoření trvale udržitelného a provozně efektivního řešení pro hostování aplikačních služeb,
- podpora provozních scénářů s vysokou dostupností a automatickým failoverem,
- integrace virtualizační platformy s existujícím IT prostředím a plánovanými systémy (ERP, CRM, POS systémy a další).

1. Základní požadavky na řešení

1.1 Rozsah hostovaných systémů

Zhotovitel je povinen navrhnout řešení, které zajistí:

- **Plně funkční virtualizační cluster** v režimu 24/7 s garantovanou dostupností
- **Implementaci virtualizační technologie** s cluster konfigurací pro vysokou dostupnost

- **Řízení virtuálních strojů** v návaznosti na aplikační požadavky a výkonnostní profily

Virtualizační platforma musí podporovat hostování subsystémů jako jsou: - ERP systém a finanční aplikace - Docházkový a personální systém - Pokladní systémy a gastro aplikace - Tiskové a souborové služby - Doménové služby (Active Directory) - Závorové a přístupové systémy - Wi-Fi management a síťové služby - Další aplikační a systémové služby dle potřeby

1.2 Typy prostředí

Virtualizační platforma musí poskytovat jednotné systémové prostředky pro provoz různých typů prostředí:

- **Produkční prostředí** – zajištění produkčního provozu kritických systémů
- **Testovací prostředí** – pro ověření funkčnosti a bezchybnosti řešení před nasazením do produkce
- **Školící prostředí** – určeno k uživatelskému seznámení se s řešením, vyzkoušení jeho funkcionalit a realizaci školení

Poznámka: Oddělení jednotlivých funkčních systémů bude realizováno prostředky virtualizace (např. VLAN, virtuální switche, izolace zdrojů).

2. Architektura virtualizačního řešení

2.1 Požadavky na architekturu

Zhotovitel musí v rámci předimplementační analýzy navrhnout architekturu, která zajistí:

- **Vysokou dostupnost (HA):**
  - Minimálně dva fyzické servery tvořící virtualizační cluster
  - Automatický failover při výpadku jednoho serveru
  - Možnost živé migrace virtuálních strojů mezi servery bez výpadku (Live Migration)
- **Odolnost proti výpadku:**
  - Eliminace Single Point of Failure (SPoF)
  - Redundantní komponenty (napájení, síťové karty, storage kontrolery)
  - Dimenzování systémových prostředků pro překlenutí výpadku jednoho serveru
- **Škálovatelnost:**
  - Možnost budoucího rozšíření o další výpočetní nody
  - Možnost navýšení operační paměti pamětí
  - Možnost navýšení úložné kapacity

2.2 Primární provozní platforma

Zhotovitel v rámci předimplementační analýzy navrhne primární virtualizační platformu zahrnující:

- **Virtualizační cluster:**
  - Minimálně 2 fyzické servery (compute nody) identické konfigurace
  - Cluster konfigurace pro vysokou dostupnost
  - Umístění v primárním datovém centru (DC1)
- **Centrální úložný systém:**
  - Sdílené úložiště pro všechny virtuální stroje
  - Redundantní kontrolery
  - Připojení přes standardizované protokoly (iSCSI, FC, nebo ekvivalent)
- **Redundantní síťová infrastruktura:**
  - Dual-home připojení serverů
  - Redundantní switche
  - Segmentace síťové komunikace (VLAN)

3. Virtualizační platforma

3.1 Požadavky na virtualizační technologii

Zhotovitel musí navrhnout a realizovat virtualizační platformu, která zajistí:

- **Podporu hypervisoru typu 1 (bare-metal):**
  - Vysoký výkon a nízká režie
  - Možnost provozu různých operačních systémů (Windows, Linux)
- **Funkce vysoké dostupnosti:**
  - Automatický restart virtuálních strojů při výpadku fyzického serveru
  - Živá migrace virtuálních strojů mezi servery (Live Migration)
  - Možnost bezvýpadkové údržby
- **Správu a monitoring:**
  - Centralizované nástroje pro správu virtuálních strojů
  - Webové nebo grafické rozhraní
  - Možnost automatizace a skriptování
- **Zabezpečení:**
  - Izolace virtuálních strojů
  - Integrace s Active Directory nebo ekvivalentem
- **Podporu kontejnerů** (volitelně):
  - Možnost provozu kontejnerových aplikací

3.2 Integrace virtualizační platformy

Zhotovitel zajistí možnost integrace s:

- **Systémem jednotné správy identit (IDM):**
  - Centralizovaná správa uživatelských přístupů

- **Nástroji pro správu a dohled:**
  - Integrace s monitorovacím systémem (SNMP, API, agenti)
  - Sběr performance dat, logů událostí
- **Systémem zálohování a obnovy:**
  - Podpora snapshotů a replikace
  - Integrace se zálohovacím softwarem
- **Bezpečnostním monitoringem:**
  - Integrace s SOC (pokud existuje)
  - Sběr auditních záznamů

4. Výpočetní nody (Compute Nodes)

4.1 Požadavky na fyzické servery

Zhotovitel musí v rámci předimplementační analýzy specifikovat parametry fyzických serverů zahrnující:

- **Architektura:**
  - x86-64 architektura
  - Montáž do 19” racku (1U nebo 2U)
- **Procesor (CPU):**
  - Počet procesorů (1 nebo 2)
  - Počet jader na procesor (minimálně 12-16 jader)
  - Frekvence (GHz)
  - Podpora virtualizace (Intel VT-x, AMD-V)
- **Operační paměť (RAM):**
  - Minimální kapacita: 256-512 GB
  - Typ paměti (DDR5 nebo novější)
  - Možnost rozšíření
- **Interní disková kapacita:**
  - Minimálně 2× SSD pro OS a hypervisor
  - RAID 1 konfigurace
  - Kapacita: 480 GB - 1 TB
- **Síťové rozhraní (LAN/SAN):**
  - Minimálně 4-6× síťové porty
  - Rychlost: 10 GbE, 25 GbE nebo vyšší
  - Optické moduly (pokud požadováno)
- **Dedikovaný management port:**
  - 1 GbE pro vzdálený management
  - KVM over IP, virtuální média

- **Napájení:**
  - 2× redundantní zdroje
  - Hot-swap
  - Účinnost: 90% a vyšší (doporučeno Platinum/Titanium)
- **Příslušenství:**
  - Ližiny pro montáž do 19” racku

4.2 Dimenzování výpočetních zdrojů

Zhotovitel provede dimenzování výpočetních zdrojů s ohledem na:

- **Počet a typ hostovaných virtuálních systémů, které jsou součástí plnění Zhotovitele**
- **Výpočetní výkon** (CPU cores, MHz)
- **Paměťové nároky** (RAM v GB)
- **Režim N+1** – schopnost překlenout výpadek jednoho serveru bez dopadu na provoz

Orientační parametry (Zhotovitel navrhne a realizuje podle skutečných potřeb): - Celkový počet virtuálních strojů: 20-50 - Celková RAM: 256-512 GB na server - Celkový CPU: 16-32 cores na server

5. Centrální úložný systém (Storage)

5.1 Požadavky na storage systém

Zhotovitel musí navrhnout a realizovat centrální úložiště, které zajistí:

- **Sdílený přístup:**
  - Přístup pro všechny servery v clusteru
  - Protokoly: iSCSI nebo Fibre Channel nebo NFS nebo SMB nebo ekvivalent
- **Redundance:**
  - Minimálně 2 kontrolery v režimu aktiv-aktiv
  - Bezvýpadkový provoz při výpadku jednoho kontroleru
- **Výkon:**
  - Dostatečný výkon pro běh všech virtuálních strojů, které jsou součástí plnění Zhotovitele nabízených Dodavatelem
  - Nízká latence
- **Kapacita:**
  - Čistá kapacita: 25-50 TB
    - Čista kapacita bez aplikace redukčních mechanismů
  - Možnost budoucího rozšíření
- **Ochrana dat:**
  - RAID 5, RAID 6 nebo ekvivalent

    - Hot-spare disky nebo kapacita
    - Deduplikace a komprese (volitelně)

5.2 Technické parametry storage

Zhotovitel v rámci předimplementační analýzy specifikuje:

- **Typ úložiště:**
    - Diskové pole (SAN)
    - Hyper-converged infrastruktura
    - Nebo ekvivalent
- **Kontrolery:**
    - Počet (minimálně 2)
    - Paměť cache (GB)
    - Režim práce (aktiv-aktiv, aktiv-pasiv)
- **Front-End konektivita:**
    - Protokol (iSCSI nebo FC nebo NFS nebo SMB)
    - Počet portů
    - Rychlost (10 GbE nebo 25 GbE nebo 32 Gb FC nebo vyšší)
- **Disky:**
    - Typ (SSD, NVMe, HDD)
    - Počet disků
    - Kapacita jednotlivých disků
    - RAID konfigurace
    - Čistá kapacita po RAID
- **Management rozhraní:**
    - Webové GUI
    - API pro automatizaci
    - Dedikovaný management port
- **Napájení:**
    - 2× redundantní zdroje
    - Hot-swap

6. Síťová infrastruktura

6.1 LAN infrastruktura

Zhotovitel musí navrhnout a realizovat redundantní LAN připojení zahrnující:

- **Core switche v primárním DC:**
    - Minimálně 2× L3 switch
    - Dual-home připojení serverů

    - Podpora VLAN pro segmentaci
    - Redundantní napájení
- **Distribuční switche v sekundárním DC** (pokud je paralelní infrastruktura součástí):
    - Redundantní připojení do core switchů

6.2 SAN infrastruktura

Zhotovitel navrhne a realizuje redundantní SAN připojení dle níže uvedených požadavků, pokud bude součástí dodávky Zhotovitele:

- **SAN fabric:**
    - Dva nezávislé SAN subnety (VLAN) pro eliminaci SPoF
    - iSCSI nebo Fibre Channel
- **Připojení:**
    - Každý server připojen do obou SAN fabric
    - Každý storage kontroler připojen do obou SAN fabric
- **Multipathing:**
    - Podpora více cest k úložišti
    - Automatický failover

7. Centrální provozní monitoring

7.1 Požadavky na monitoring

Zhotovitel musí navrhnout a realizovat centrální monitorovací systém pro:

- **Dohled nad infrastrukturou:**
    - Fyzické servery (compute nody)
    - Virtuální stroje
    - Storage systém
    - Síťové prvky
- **Sledované metriky:**
    - Dostupnost (uptime/downtime)
    - Výkon (CPU, RAM, disk I/O, network)
    - Kapacita (volné místo, trendy růstu)
    - Chybové stavy
- **Funkcionalita:**
    - Centralizované WebGUI rozhraní
    - Automatizované zasílání notifikací při nestandardním chování
    - Uchovávání historických dat pro kapacitní plánování
    - Integrace s ticketovacím systémem (volitelně)

7.2 Technické řešení monitoringu

Zhotovitel navrhne a realizuje monitorovací systém s následujícími vlastnostmi:

- **Platforma:**
  - Opensource nebo komerční řešení
  - Škálovatelnost
- **Protokoly:**
  - SNMP, ICMP, HTTP, SSH, SYSLOG
  - API jednotlivých systémů
  - Agenti na serverech
- **Architektura:**
  - Centrální monitoring server
  - Možnost proxy serverů pro distribuované prostředí (pokud potřeba)
- **Výkonové nároky:**
  - Zhotovitel provede sizing dle počtu sledovaných metrik
  - Orientačně: 10 000 - 20 000 metrik
- **Implementace:**
  - Virtuální server v rámci virtualizační platformy
  - Parametry VM (Zhotovitel specifikuje): CPU, RAM, HDD, OS, databáze

8. Licencování

8.1 Požadavky na licencování

Zhotovitel v rámci předimplementační analýzy předloží návrh licencování zahrnující:

- **Virtualizační platforma:**
  - Typ licence (perpetual, subscription, OEM)
  - Metrika licencování (procesory, jádra, servery)
  - Počet licencí
  - Zhotovitel navrhne licenční model umožňující provoz plánovaného počtu VM (20-50) s rozumnou rezervou pro růst (Standard edition / Datacenter edition).
- **Operační systémy virtuálních strojů:**
  - Licence pro hostované OS (Windows Server, Linux)
  - Pokrytí všech plánovaných virtuálních strojů
  - Licence typu Datacenter vs. Standard (porovnání)
- **Databázové servery** (pokud součástí):
  - Pokud jsou součástí databázových serverů databáze dodané Zhotovitelem, musí být tyto databáze plně licenčně zajištěny v rámci dodávky. Požadavky třetích stran na doinstalaci nebo rozšíření databáze budou řešeny

prostřednictvím samostatných rozvojových požadavků a mohou podléhat samostatnému licencování.
    - Metrika licencování (jádra, uživatelé, CAL)
- **Maintenance a podpora:**
    - Nárok na aktualizace a opravy
    - Frekvence aktualizací
    - Podpora nových verzí
- **Dopady při ukončení licence:**
    - Funkčnost systému po ukončení licence
    - Možnost migrace na jiné řešení

8.2 Porovnání licenčních modelů

Zhotovitel je oprávněn pro své řešení zvolit některý z následujících licenčních modelů:

- **Datacenter vs. Standard edice:**
    - Datacenter: neomezený počet VM, vyšší cena
    - Standard: omezený počet VM, nižší cena
- **OEM vs. Volume Licensing:**
    - OEM: vázáno na HW, nižší cena
    - Volume: přenositelné, možnost SA (Software Assurance)

9. Bezpečnost virtualizovaného prostředí

9.1 Bezpečnostní opatření

Zhotovitel musí zajistit:

- **Řízení přístupu (RBAC):**
    - Definice rolí a oprávnění
    - Integrace s Active Directory
- **Izolace virtuálních strojů:**
    - Síťová izolace (VLAN, virtual switche)
    - Izolace zdrojů
- **Šifrování:**
    - Šifrování komunikace (TLS/SSL)
    - Šifrování úložiště (volitelně)
- **Auditní záznamy:**
    - Sběr a archivace logů
    - Integrace s SIEM (pokud existuje)
- **Ochrana hypervisoru:**
    - Bezpečnostní aktualizace

    - Hardening dle best practices
- **Antivirus/antimalware:**
    - Ochrana fyzických serverů
    - Ochrana virtuálních strojů

10. Implementace a předání do provozu

10.1 Fáze implementace

Zhotovitel zajistí komplexní implementaci v následujících krocích:

10.1.1 Návrh architektury

- Kickoff meeting
- Odborná analýza pro přípravu navazujících implementačních kroků
- Návrh topologie virtuálních strojů a jejich optimální rozložení
- Návrh architektury řešení

10.1.2 Dodávka a montáž

- Dodávka všech hardwarových komponent
- Montáž do racků
- Zapojení do sítě a storage

10.1.3 Instalace a konfigurace

- Instalace virtualizační platformy
- Konfigurace clusteru pro vysokou dostupnost
- Konfigurace storage a SAN připojení
- Konfigurace síťové infrastruktury (VLAN, virtual switche)
- Instalace monitorovacího systému

10.1.4 Implementace postupů pro HA

- Konfigurace automatického failoveru
- Implementace postupů pro živou migraci
- Konfigurace automatického obnovení služeb při výpadku

10.1.5 Migrace a nasazení systémů

- Migrace stávajících systémů (pokud existují)
- Instalace nových virtuálních strojů
- Konfigurace jednotlivých aplikací

10.1.6 Integrace

- Integrace s nástrojem pro správu a dohled
- Integrace se systémem zálohování
- Integrace s bezpečnostním monitoringem
- Integrace s IDM systémem

10.1.7 Testování

- Testování funkčnosti virtualizačního clusteru
- Testování vysoké dostupnosti (failover, live migration)
- Testování výkonu a kapacity
- Podpora scénářů pro zálohování a obnovu dat

10.1.8 Dokumentace a školení

- Zpracování technické dokumentace
- Provozní příručky
- Školení administrátorů

10.1.9 Akceptace a předání

- Akceptační testy
- Předání do produkčního provozu

10.2 Časový rámec implementace

Zhotovitel v rámci předimplementační analýzy předloží harmonogram implementace s konkrétními milníky a termíny odpovídající výše uvedeným fázím a termínům dle Smlouvy.

11. Vymezení rozsahu dodávky

11.1 Co je součástí dodávky

- Návrh architektury řešení
- Dodávka a instalace všech hardwarových a softwarových komponent
- Konfigurace virtualizační platformy
- Konfigurace clusteru pro vysokou dostupnost
- Konfigurace storage a SAN
- Konfigurace síťové infrastruktury
- Instalace monitorovacího systému
- Migrace stávajících systémů (pokud existují)
- Školení administrátorů
- Technická dokumentace a provozní příručky
- Konzultační a metodická podpora
- Provozní podpora dle SLA

11.2 Požadavky na součinnost Objednatele

- Zajištění přístupů k systémům a infrastruktuře
- Nominování odpovědných osob
- Účast na implementačních aktivitách
- Poskytnutí informací o aplikačních systémech a jejich požadavcích

- Zajištění koordinace s dodavateli dalších systémů (síť, bezpečnost)

12. Požadované výstupy od Zhotovitele

12.1 Projektová dokumentace

- **Detailní návrh architektury** virtualizačního řešení s odůvodněním volby technologií
- **Diagram architektury** (topologie, tok dat, redundance)
- **Dimenzování výpočetních zdrojů** s výpočtem kapacity CPU, RAM, storage
- **Implementační plán** s časovým harmonogramem a milníky
- **Specifikace všech komponent** včetně technických parametrů (CPU, RAM, HDD, síťové rozhraní, redundance)

12.2 Provozní dokumentace

- Technická dokumentace systému a konfigurace
- Topologie virtuálních strojů
- Provozní příručky pro administrátory
- Postupy pro živou migraci a automatické obnovení služeb
- Postupy pro zálohování a obnovu dat
- Disaster Recovery plán (pokud aplikovatelné)

12.3 SLA a záruky

- SLA dle přílohy č. 5 Smlouvy
- Záruční podmínky na všechny dodané komponenty dle Smlouvy
- Postupy pro řešení poruch a výpadků

13. Kompatibilita a integrace

Řešení musí být navrženo jako:

- **Škálovatelná a rozšiřitelná platforma** s možností budoucího růstu
- **Využívající otevřené a standardizované technologie** pro snadnou integraci
- **Auditovatelná** v rámci správy a přístupu
- **Centralizovaně řízená** prostřednictvím jednotného nástroje
- **V souladu s bezpečnostními normami** a legislativními požadavky (např. GDPR, Zákon o kybernetické bezpečnosti)

Řešení musí být kompatibilní s: - Plánovanými technologiemi a hardwarem Objednatele - Systémy pro zálohování a obnovu - Datovým úložištěm - Správou systémových služeb - Síťovou infrastrukturou - Bezpečnostním monitoringem

14. Koordinace a komunikace

Požaduje se komunikace a koordinace s:

- **Správcem sítě a ICT infrastruktury Objednatele** pro zajištění plynulé integrace a kompatibility řešení
- **Dodavatelem kybernetické bezpečnosti** pro implementaci technologických a organizačních opatření v souladu s bezpečnostními standardy a požadavky na ochranu informačních aktiv
- **Dodavateli dalších systémů** (ERP, CRM, storage, zálohovací systémy) pro zajištění celkové kompatibility

7. Služby návrhu a implementace WiFi datové sítě – popis požadovaného řešení, stavu a potřeb Objednatele

Objednatel má zájem o návrh a realizaci infrastruktury WiFi datové sítě, která bude tvořit nedílnou součást technologického prostředí multifunkční haly ARENA BRNO, a.s. Cílem je vytvořit robustní a bezpečné bezdrátové řešení s plnou integrací do stávající a plánované síťové architektury, podporující interní provozní potřeby.

Objednatel stanovuje, že předmětem dodávky je dodání maximálně 80 ks AP (bez rezervních kusů) a přibližný objemový návrh rozmístění AP; Smlouva obsahuje ujednání o možnosti rozšíření dodávky o další AP na základě předimplementační analýzy nebo na základě provozní zkušenosti dle podmínek uvedených ve Smlouvě.

Zhotovitel předloží v rámci předimplementační analýzy požadavek na doplnění chybějících koncových zásuvek UTP kabeláže (které nesplňují stavební připravenost kabeláže pro maximálně 5 metrů připojovacího UTP kabelu bez nutnosti stavebních úprav, tvorby prostupů, tvorby požárních ucpávek, tvorby žlabů – viz dále) v budově ke konkrétním AP a to tak, že předloží definici plánovaného umístění AP a navržené místo požadované zásuvky RJ45.

Cílem je:

- zajištění stabilního a bezpečného WiFi pokrytí v dále specifikovaných prostorách multifunkční ARENY BRNO (haly)
- podpora odděleného přístupu pro různé skupiny uživatelů (provoz, personál, technologická zařízení s WiFi konektivitou, návštěvníci),
- centralizovaná správa WiFi infrastruktury s podporou monitoringu a přístupového řízení,
- integrace s plánovanými systémy kybernetické bezpečnosti, dohledového centra a správy identit.

Zhotovitel je povinen navrhnout řešení, které zajistí:

- Úplné Pokrytí wifi způsobem a v rozsahu očekávaných technických parametrů Etapy 1

a bude obecně připraven na technologické rozšíření pro splnění parametrů Etapy 2 (viz níže),

- provozní dostupnost bezdrátové sítě pro běžné i kritické provozní systémy,
- řízení přístupů prostřednictvím přihlašovacích a autentizačních mechanismů (např. captive portal, integrace IDM),
- oddělené SSID s možností definování šířky pásma, prioritizace a omezení dle skupin uživatelů,
- řízení přístupových práv přes integraci na existující IDM systém nebo jeho rozhraní (např. LDAP, API),
- přehledný dohled a správu WiFi prostředí prostřednictvím centrálního nástroje.
- z důvodu stability sítě Objednatel doporučuje nepoužít Spanning tree protokol / technologií,
- bude podporován protokol IPv6.

Součástí návrhu v rámci předimplementační analýzy musí být rovněž:

- vyhotovení útlumového plánu a návrh umístění přístupových bodů (AP) dle reálného členění prostor,
- návrh kmitočtové koordinace a optimalizace výkonu AP za účelem minimalizace rušení a zajištění plynulého provozu,
- začlenění řídicí jednotky (např. kontroler/server) do síťové infrastruktury PROVozní datové sítě včetně specifikace způsobu správy a zálohování konfigurace,
- návrh kabeláže pro připojení AP do stávající metalické/optické páteře a identifikace napájecích požadavků (PoE apod.) ve vztahu k návrhu a dodávce aktivních prvků PROVozní datové sítě (jiná část dodávky Zhotovitele),
- plán fyzického osazení a identifikace vhodných již stavbou připravených zásuvek horizontální metalické (UTP) sítě a dalších připojovacích bodů (racky, zásuvky, switche apod.).

Architektura musí být v souladu s koncepcí jednotné infrastruktury a nesmí být v rozporu se síťovými, serverovými a bezpečnostními technologiemi Objednatele, jež jsou součástí této dodávky anebo infrastruktury stavby. Návrh musí zohlednit proveditelnost možného budoucího rozšíření dle Etapy 2. Návrh musí zohlednit možnost správy z jednoho místa, tedy musí obsahovat administrační rozhraní (WiFi controlleru). Kompletní správu ve formě přidělování přístupů a služeb uživatelům (jejich zařízením), nebo změnu zapojení do jiných VLAN v rámci PROV sítě si musí být schopen zajistit během provozu Objednatel prostřednictvím vlastního odborného pracovníka (viz dále “zaškolení správců systému“).

Koordinace a integrace:

- Zhotovitel bude koordinovat návrh a instalaci s dodavateli systémů kybernetické bezpečnosti (SOC), správy identit (IDM), a infrastruktury (LAN, serverovna),

- řešení musí umožnit integraci s dohledovým a monitoring systémem Objednatele,
- Objednatel požaduje spolupráci při konfiguraci přístupových práv, přístupového rozhraní a síťových segmentů včetně VLAN.

Součástí dodávky a realizace bude:

- Součástí dodávky bude obecný projekt pro pokrytí se splněním parametrů Etapy 2, tedy pro hypotetické poskytnutí konektivity i pro návštěvníky (13.000 osob se započítáním všech typů soudobostí) s tím, že řešení s parametry Etapy 1 by mělo být jeho podmnožinou tam, kde to je logicky a technicky vhodné (tedy AP se mohou instalovat podle projektu Etapy 1 na místa, kam by se instalovala i dle projektu Etapy 2 - pokud je to provozně vhodné).
- vypracování realizační projektové dokumentace s rozmístěním zařízení,
- dodávka a instalace aktivních prvků bezdrátové infrastruktury (AP, řídicí prvky, potřebná kabeláž),
- konfigurace SSID, šifrování, QoS parametrů a přístupových pravidel,
- testování pokrytí, validace výkonu a zajištění dokumentace skutečného stavu,
- zaškolení správců systému na straně Objednatele a předání provozní dokumentace.

Řešení WiFi infrastruktury bude koncipováno jako plně integrovaný prvek provozního prostředí haly, zajišťující konektivitu pro uživatele, zařízení a provozní systémy s důrazem na bezpečnost, škálovatelnost a snadnou správu.

Požadované technické parametry

Etapa 1

- Typově se očekává, že pro WiFi síť bude celkem využito řádově 200-800 Mbps konektivity do internetu. (Údaje uvedené níže nelze jen prostě sčítat, protože pravděpodobnost naplnění požadavků na 100 % je minimální a vždy existuje i soudobost mezi sítěmi.)
- WiFi sítě:
    - Počet WiFi sítí až 20 plně roamovaných sítí s odlišnými SSID:
    - Požadovaný počet souběžně připojených zařízení se bude v jednotlivých sítích výrazně lišit podle typu sítě (viz výkresová dokumentace v příloze).
        - 5-8 Produkčních sítí - pro zařízení v těchto sítích určených pro menší počet uživatelů/zařízení lze předpokládat požadavek na konektivitu 20 Mbps per uživatel pro 1-20 uživatelů v soudobosti 0,5. Typickým uživatelem je osoba s notebookem. Počet sítí (SSID) může být vyšší naopak s menším počtem uživatelů). Na nákresech výkresové dokumentace jde o plochy vyznačené modrou plochou.
        - 1-2 Support sítě - pro zařízení v sítích pro větší počet uživatelů/zařízení lze předpokládat požadavek na konektivitu 250 kbps per uživatel pro 70 uživatelů v soudobosti 0,5. Typickým uživatelem je čtečka vstupenek,

platební terminál apod. Plocha pokrytí jednotlivých AP pro Support sítě musí mít v prostoru západního a východního vstupního foyeru vytvořené přesahy pokrytí (duplicity) z důvodů redundance při případném výpadku jednotlivých AP. Na výkresové dokumentaci jde o plochy vyznačené žlutou plochou.

        - 1-2 retailové sítě - pro zařízení nájemců komerčních prostor lze předpokládat požadavek na konektivitu pro max 30 osob per síť s konektivitou 5 Mbps v soudobosti 0,1 v samostatných SSID. Na výkresové dokumentaci jde o plochy vyznačené zelenou plochou.
    - V některých sítích budou nad rámec poskytování internetových služeb poskytovány i vnitřní datové služby (lokální).
    - V přiložených půdorysech výkresové dokumentace je obsažen i výkres "7-Roof" s vyobrazením servisních lávek pod ocelovou konstrukcí střechy. Na těchto lávkách předpokládáme zřízení sektorových WiFi AP se směrovými anténami pro pokrytí vnitřního objemu haly (tedy směrem dolů). Zde předpokládáme klienty typu mobil, tablet, notebook na ca 10 SSID (na různých kanálech) především z Produkčních a Support sítí.
    - Na půdorysu 1NP je ve výkresové dokumentaci znázorněna potřeba, aby pokrytí bylo v místě vybraných vstupních a evakuačních dveří také v ploše bezprostředně před halou (2-5 m, pro potřeby čteček vstupenek).
    - Na půdorysech jsou červenými značkami znázorněny přibližné modelové umístění WiFi AP dle předběžného návrhu Objednatele. Z nich vyplývá předpokládaný stropový počet WiFi AP pro nabídkovou cenu.
    - Na půdorysech jsou vyznačeny plochy pro pokrytí pomocí 1-2 Gastro sítí – pro zařízení v sítích pro větší počet uživatelů/zařízení lze předpokládat požadavek na konektivitu 250 kbps per uživatel pro 30 uživatelů v soudobosti 0,5. Typickým uživatelem je platební terminál apod. Na výkresové dokumentaci jde o plochy vyznačené růžovou plochou. POKRYTÍ TĚCHTO PLOCH NENÍ VE VÝCHOZÍM STAVU POŽADOVÁNO a bude v případě potřeby řešeno v rámci předimplementační analýzy doplněním WiFi AP.

Součástí dodávky je UTP kabeláž pro připojení AP k Eth zásuvkám v objektu. Lze mít za to, že průměrná délka kabeláže od Ethernetové zásuvky instalované v objektu k jednotlivým AP je do 5 kabelových metrů bez nutnosti stavebních úprav, tvorby prostupů, tvorby požárních ucpávek, tvorby žlabů. Kde tento požadavek nebude odpovídat skutečnosti, bude doplněn Objednatelem a požadavky na tyto změny vzniknou v rámci předimplementační analýzy – viz výše. Patchcordy v IDF jsou také součástí dodávky. Jiná kabeláž není pro předmětnou realizaci potřeba.

Součástí dodávky je řídicí controller (bude umístěn v objektové serverovně), dále pak SW a potřebné licence. Controller může být umístěn i na objektovém virtualizovaném serveru.

Etapa 2

- Konektivita do internetu by vzrostla o 1-2 GB
- přibyla by skupina (skupiny) SSID pro běžné návštěvníky, přihlašování přes Radius server nebo i bez přihlašování
- počet návštěvníků až 13.000 ve vnitřním objemu haly
- počet návštěvníků až 6.000 v chodbách 1NP+2NP
- počet návštěvníků až 2.000 v chodbách 3NP
- počet návštěvníků až 1.000 v chodbách 4NP
- počet návštěvníků až 2.500 v chodbách 5NP

8. Provozní datová síť ARENA BRNO

Tato kapitola popisuje požadovaný princip řešení PROVozní datové sítě na struktuře Základní datové sítě (optická kabeláž) a to především fyzické propojení optické kabeláže s aktivními prvky (switche) v patchroomech (IDF), a s navazující horizontální metalickou kabeláží UTP.

Cílem je popsat Aktivní prvky (switche, core switche, firewall atd.), které je nutno instalovat do stávající infrastruktury optické a metalické kabeláže multifunkční haly ARENA BRNO.

Součástí této kapitoly je:

- Principiální popis stávající infrastruktury (není součástí dodávky)
- Topologie sítě určené pro většinu datového provozu v budově (síť PROV)
- Z důvodu stability sítě Objednatel navrhuje nepoužít Spanning tree protokol / technologií
- Bude podporován protokol IPv6
- Výčet prvků a jejich vlastností
    - switche, core switche, firewall
    - racky (není součástí dodávky)
    - patchkabely optické i metalické

1. Principiální popis sítě

- Topologicky je Datová síť tvořena
    - vertikální (optickou) kabeláží
      popsanou v dokumentaci pod názvy **Základní datová síť** - popis a topologie vč. definice uzlů (místností) MDF a IDF, **schéma OK** Základní datové sítě v Příloze č. 4 níže.
    - horizontální (metalickou) kabeláží
- Fyzicky a organizačně je síť dále tvořena slaboproudými rozvodnami (uzly) s označením MDF a IDF. Tyto rozvodny, umístěné v jednotlivých patrech budovy, jsou vybaveny slaboproudými rozvaděči (racky):
    - půdorysné umístění slaboproudých rozvoden vč. rozmístění racků viz Příloha č. 5 “Souhrn půdorysů MDF a IDF”
    - kompletní seznam racků - viz Příloha č. 1 “Seznam racků” níže
    - modelový seznam aktivních prvků (switchů) - viz Příloha č. 3 “Modelový příklad aktivních prvků” níže
    - rozvaděče (racky) jsou vybaveny následujícími prvky (podrobněji o vystrojení jednotlivých racků viz kapitola Pasivní prvky sítě):
        - optické vany (ODF) - počet vychází ze schématu **Základní datové sítě**

        - patchpanely horizontální metalické kabeláže - počet vychází z dokumentace DPS pro provedení zásuvek v jednotlivých patrech
        - vertikální vyvazovací lišta (pro racky 45U)
        - horizontální vyvazovací panely pro patchkabely - počet viz tabulka dále
    - rozvaděče (racky) je nutno dovybavit následujícími prvky (podrobněji o vystrojení jednotlivých racků viz kapitola Pasivní prvky sítě):
        - patchkabely optické seznam viz níže Příloha č. 2
        - patchkabely metalické (UTP) seznam viz níže Příloha č. 2
        - aktivní prvky (switche + optické transcievery)
        - router (nebo core switche)
        - firewall
        - napájecí lišta PDU pro dodané aktivní prvky

2. Aktivní prvky

Objednatel požaduje zprovoznění PROVozní datové sítě (dále také jako “PROV”) propojující běžná provozní zařízení budovy:

- přístupové systémy pro návštěvníky (turnikety, bezdrátové čtečky…)
- platební terminály vč. bezdrátových
- provozní počítače, notebooky
- IP set-top-boxy systému DigitalSignage
- Wi-Fi AP pro nejrůznější bezdrátová zařízení a pro zřízení konektivity pomocí Wi-Fi klienta
- atd.

Aktivními prvky sítě rozumíme všechny switche a core switche, router, firewall apod.

Počet portů aktivních prvků je uveden v tabulce č. 3 této přílohy. Pokud bude provozní požadavek v budoucnu vyšší, bude řešen přidáním aktivních prvků.

Požadované vlastnosti prvků PROV-ozní sítě

Access switche

Požadované vlastnosti výchozích access switchů (dále SW_Typ_1):

- min 4x SFP+ uplink/stacking porty
- min 1 napájecí zdroj
- stohovatelné
- první switch v IDF: 48port PoE+ s minimálním PoE výkonem 450W

Požadované vlastnosti rozšiřujících access switchů (dále SW_Typ_2):

- jako SW_Typ_1 ale nemusí být PoE

Požadované vlastnosti access switche v IDF 6.1 (dále SW_Typ_3):

- 4-8x SFP28 uplink porty
- min 1 napájecí zdroj
- zbytek portů metalických nebo optických - min 16 portů, min 2,5 Gbps per port

Požadované vlastnosti optického access switche v MDF.1 (dále SW_Typ_4):

- minimálně 24x 1G/10G SFP/SFP+
- minimálně 4-8x SFP28 uplink porty
- min 1 napájecí zdroj

CORE switche

Požadované vlastnosti CORE switchů (dále Core_SW):

- 4-8x SFP28 uplink porty
- min 32x SFP+
- min 1 napájecí zdroj

Schéma zapojení a výčet aktivních prvků

Schéma zapojení prvků jednotlivých sítí vychází z topologie optické kabeláže **Základní datové sítě**.

- Schéma zapojení **PROV** sítě - viz níže Příloha č. 4 “PROV-ozní síť (schéma)”
- Modelový seznam použitých aktivních prvků - switchů - viz níže Příloha č. 3 “Modelový příklad aktivních prvků”

Rozměrová kompatibilita

Montážní rozměry navržených konkrétních typů switchů musí být v souladu s půdorysnými rozměry racků aby nedošlo ke kolizi - konkrétní typy switchů je možné namontovat do konkrétního racku - viz Příloha č. 1 “Seznam racků”

3. Pasivní prvky sítě

Seznam racků

V příloze je definován souhrn všech racků, které odpovídají půdorysným zákresům.

V seznamu racků jsou pro úplnost vyjmenovány i racky AV, DMX, CCTV atd. (v seznamu přeškrtnuté), které nejsou součástí tohoto projektu a nelze je využít.

Předpis pro umístění aktivních a pasivních prvků v rámci racku

Z důvodu efektivity patchování a ekonomiky délek patchkabelů je nutno dodržet následující obecný princip umístění prvků:

Rack “IDF SK” 45U (univerzálně)

optické vany (ODF)	vyvazovací lišta
vyvazovací panel	
switch TECH sítě	
vyvazovací panel	
patchpanel TECH portů	
první polovina ostatních patchpanelů metalika (střídané s vyvazovacími panely v poměru 2patch/1vyvazovací panel)	
vyvazovací panel	
3U blok: switche PROV sítě (1-2) + 1 až 2 1U záslepky	
vyvazovací panel	
druhá polovina ostatních patchpanelů metalika (střídané s vyvazovacími panely v poměru 2patch/1vyvazovací panel)	
ponechat prázdné (zbytek, různá výška)	
1x police hluboká	
2x PDU	
2U ponechat volné	

Rack “ODF” MDF.1 45U (centrum optické kabeláže)

2U optické vany 24xLC-D Základní datové sítě (ODF)	vyvazovací lišta
vyvazovací panel	
optický access switch PROV sítě (MDF.1b)	
vyvazovací panel	
14x optické vany 24xLC-D Rezervní datové sítě (ODF) - střídané s vyvazovacími panely v poměru 2ODF/1vyvazovací panel	
ponechat prázdné (zbytek, různá výška)	
1x police hluboká	
2x PDU	
2U ponechat volné	

Pozn: v tomto racku bude zakončení OK v počtu 4x24v Základní datové sítě a 40x8v Rezervní datové sítě

Rack “IDF SK” 45U v MDF.1

vyvazovací panel	vyvazovací lišta
switch TECH sítě	
vyvazovací panel	
patchpanel TECH portů	
první polovina ostatních patchpanelů metalika (střídané s vyvazovacími panely v poměru 2patch/1vyvazovací panel)	
vyvazovací panel	
3U blok: switch PROV sítě (MDF.1a) + 2 1Uzáslepky	
vyvazovací panel	
druhá polovina ostatních patchpanelů metalika (střídané s vyvazovacími panely v poměru 2patch/1vyvazovací panel)	
ponechat prázdné (zbytek, různá výška)	
1x police hluboká	
2x PDU	
2U ponechat volné	

Rack “ICT” 32U v MDF.1

1U CPU server DALI (dodávka stavby)
ponechat prázdné (zbytek, různá výška)
1x police hluboká
2x PDU
2U ponechat volné

Rack č. 4 “ICT” 45U v MDF.2 a ”ICT” 32U v MDF.1

2U CPU IP tel ústředna (dodávka stavby)
3U (dodávka stavby)
7U prostor pro klávesnici a monitor (dodávka stavby)
1x police hluboká
ponechat prázdné (zbytek, různá výška)
1x police hluboká
2x PDU
2U ponechat volné

Rack č. 5 “IDF SK” 45U v MDF.2

vyvazovací panel
switch TECH sítě
vyvazovací panel
patchpanel TECH portů
první polovina ostatních patchpanelů metalika (střídané s vyvazovacími panely v poměru 2patch/1vyvazovací panel)
vyvazovací panel
3U blok: switch PROV sítě (MDF.2) + 2 1Uzáslepky
vyvazovací panel
druhá polovina ostatních patchpanelů metalika (střídané s vyvazovacími panely v poměru 2patch/1vyvazovací panel)
ponechat prázdné (zbytek, různá výška)
1x police hluboká
2x PDU
2U ponechat volné

Rack č. 6 v MDF.2 - zakončení optiky

vyvazovací panel
19x optické vany 24xLC-D Základní datové sítě (ODF)- - střídané s vyvazovacími panely v poměru 2ODF/1vyvazovací panel
vyvazovací panel
2x optický access switch TECH sítě (CORE1 a CORE2)
vyvazovací panel
2x optický access switch PROV sítě (CORE1 a CORE2)
vyvazovací panel
ponechat prázdné (zbytek, různá výška)
1x police hluboká
2x PDU
2U ponechat volné

Pozn: v tomto racku bude zakončení OK v počtu 17x24v Základní datové sítě

4. Seznam Příloh

- **Příloha č.1 - Seznam racků** - výčet všech racků dle typů, jejich počet a základní technické vlastnosti
- **Příloha č. 2 - Pasivní prvky - patchcordy**
- **Příloha č. 3 - Modelový příklad aktivních prvků**
    - PROV-ozní síť - modelový příklad aktivních prvků Provozní sítě vč. přehledu předběžného předpokládaného počtu instalovaných a pravděpodobně použitých portů horizontální kabeláže v daném bodě sítě
    - SFP transceivery pro PROV-ozní síť
- **Příloha č. 4 - Schémata**
    - **PROV-ozní síť** (schéma) - modelové schéma zapojení aktivních prvků Provozní sítě vč. základních informací o použitém aktivním prvku či prvcích (stackované switche) v daném bodě sítě a o předpokládaném počtu dostupných a obsluhovaných portů horizontální kabeláže v daném bodě sítě
- **Příloha č. 5 – Půdorysy MDF a IDF**
    - Samostatný dokument
- **Příloha č. 6 – Modelové umístění WiFi AP**
    - Na půdorysech jsou červenými značkami znázorněny přibližné modelové umístění WiFi AP dle předběžného návrhu investora. Z nich vyplývá předpokládaný stropový počet WiFi AP pro nabídkovou cenu.
    - Přiloženo i jako samostatné dokumenty

Příloha č. 1: Seznam racků

ozn.	místnost	určení	rozměr	typ
MDF.1	Techn. centrum	IDF SK	800x800 45U	A
	ODF	800x800 45U		A
	~~CCTV~~	~~600x600 12U~~		~~L~~
	ICT	600x600 32U		G
	ODF OPS	600x600 12U		M
	ODF OPS	600x600 12U		M
	ODF OPS	600x600 12U		M
	ODF OPS	600x600 12U		M
MDF.2	Velín	ODF	800x800 45U	A
		IDF SK	800x800 45U	A
		ICT	800x800 45U	A
		~~CCTV~~	~~800x800 45U~~	~~B~~
		~~CCTV~~	~~800x800 45U~~	~~B~~
		~~CCTV~~	~~800x800 45U~~	~~B~~
IDF.-1.1	rack SPORT	IDF SK	800x800 45U	A
		~~CCTV~~	~~600x600 12U~~	~~L~~
IDF.-1.2	rack KULTURA	IDF SK	800x800 45U	A
		~~CCTV~~	~~600x600 12U~~	~~L~~
		~~AV~~	~~?~~	~~AV~~
IDF.-1.3	rack SATNA_HC	IDF SK	600x600 32U	F
IDF.1.1	rack 1A	IDF SK	800x800 45U	A
		~~CCTV~~	~~600x600 12U~~	~~L~~
		~~AV~~	~~?~~	~~AV~~
IDF.1.2	rack 1B	IDF SK	800x800 45U	A
		~~CCTV~~	~~600x600 12U~~	~~L~~
		~~DMX~~	~~?~~	~~AV~~
IDF.1.3	rack 1C	IDF SK	800x800 45U	A
		~~CCTV~~	~~600x600 12U~~	~~L~~
		~~DMX~~	~~?~~	~~AV~~
IDF.1.4	rack 1D	IDF SK	800x800 45U	A
		~~CCTV~~	~~600x600 12U~~	~~L~~
		~~AV~~	~~?~~	~~AV~~
IDF.3.1	rack C. REVERS	IDF SK	600x600 32U	G
		~~CCTV~~	~~600x600 12U~~	~~L~~
		~~AV~~	~~?~~	~~AV~~
IDF.3.2	rack COMPLEX	IDF SK	600x600 32U	G
		~~CCTV~~	~~600x600 12U~~	~~L~~
		~~AV~~	~~?~~	~~AV~~
IDF.3.3	rack OFFICE_3NP	IDF SK	800x800 45U	B
IDF.4.1	rack OFFICE_4NP	IDF SK	600x600 32U	F
IDF.5.1	rack 5A	IDF SK	800x800 45U	A
		~~CCTV~~	~~600x600 12U~~	~~L~~
		~~DMX~~	~~?~~	~~AV~~
IDF.5.2	rack 5B	IDF SK	800x800 45U	A
		~~CCTV~~	~~600x600 12U~~	~~L~~
		~~DMX~~	~~?~~	~~AV~~
IDF.5.3	rack 5C	IDF SK	800x800 45U	A
		~~CCTV~~	~~600x600 12U~~	~~L~~
		~~DMX~~	~~?~~	~~AV~~
IDF.5.4	rack 5D	IDF SK	800x800 45U	A
		~~CCTV~~	~~600x600 12U~~	~~L~~
		~~DMX~~	~~?~~	~~AV~~
IDF.6.1	SERVEROVNA_AV	IDF SK	800x800 45U	A
		~~CCTV~~	~~600x600 12U~~	~~L~~
		~~CCTV~~	~~600x600 12U~~	~~L~~
IDF.6.2	SERVEROVNA_2	IDF SK	800x800 45U	A
IDF.6.3	rack PRESS_A	IDF SK	600x600 32U	F
	~~AV~~	~~?~~	~~AV~~	
PM AV	rack PRESS_B	~~AV~~	~~?~~	~~AV~~
IDF.7.1	rack ROOF	IDF v AV	?	AV
		~~CCTV~~	~~600x600 12U~~	~~L~~

Seznam racků dle typů:

typ	ks	rozměr	Vybavení
A	**17**	800x800 45U	Perforované dveře 80% přední i zadní, bez bočnic, vertikální vyvazovací lišta 1x
B	**4**	800x800 45U	uzavřený celoplechový s ventilací, vertikální vyvazovací lišta 1x
F	**3**	600x600 32U	uzavřený s bočnicemi, skleněné dveře, ventilátor
G	**3**	600x600 32U	Perforované dveře 80% přední i zadní, bez bočnic
L	**15**	600x600 12U	uzavřený celoplechový s ventilací - **určeno pro CCTV**
M	**4**	600x600 12U	uzavřený celoplechový s ventilací dozadu/do boku
AV			dodávka projektu AV sítě

Seznam racků dle určení:

- **ODF-** primárně určeno pro zakončení kabeláže optické sítě (možnost instalace core switchů)
- **IDF SK -** primárně určeno pro zakončení horizontální metalické kabeláže, access switche
- **CCTV -** určeno výhradně pro potřeby CCTV sítě!
- **ICT -** určeno primárně pro vnitřní ICT technologie investora (servery, firewally, úložiště…)
- **ODF OPS -** určeno výhradně jako zakončení optické kabeláže přicházející z venkovního prostředí (optika providerů a třetích stran)
- **AV -** racky instalované stavbou v rámci dodávky AV sítě a příbuzných technologií (není součástí dodávky popsané v této zprávě)

Příloha č. 2: Patchcordy

Následující tabulky obsahují seznam všech metalických a optických patchcordů. Jde o seznam kabelů, které Objednatel požaduje jako součást dodávky (provozní kabeláž) nad rámec kabeláže nezbytné pro propojení Zhotovitelem dodávaných technologií (servery, switche, WiFi atp):

Seznam patchcordů sítě PROV

určení	popis	ks
UTP patchcordy		
IP telefony Provozní	Patch kabel UTP cat.6A 3m žlutý	50
-”-	Patch kabel UTP cat.6A 5m žlutý	50
PROV síť na straně IDF	Patch kabel UTP cat.6A 2m šedý	400
-”-	Patch kabel UTP cat.6A 1m šedý	1000
-”-	Patch kabel UTP cat.6A 0,5m šedý	100
PROV síť na straně DS/wifi	Patch kabel UTP cat.6A 1m šedý	500
PROV na straně PC apod.	Patch kabel UTP cat.6A 2m šedý	300
-”-	Patch kabel UTP cat.6A 3m šedý	300
-”-	Patch kabel UTP cat.6A 5m šedý	200
Optické patchcordy:		
patchování mezi ICT-ODF a AVT-ODF	Patch kabel SM, 9/125, LC/APC - E2000/APC, simplex 2 m	10
-”-	Patch kabel SM, 9/125, LC/APC - E2000/APC, simplex 5 m	10
-”-	Patch kabel SM, 9/125, LC/APC - E2000/APC, simplex 10 m	10
patch z AVT-ODF do pressA switche	Patch kabel SM, 9/125, LC/PC - E2000/APC, simplex, 3m	5
Patche v rámci ODF (hlavně v MDF1)	Patch kabel SM, 9/125, LC/APC - LC/APC, simplex, 2m	85
Patche z ODF do switchů	Patch kabel SM, 9/125, LC/PC - LC/APC, simplex, 2m	20
-”-	Patch kabel SM, 9/125, LC/PC - LC/APC, simplex, 5m	15

Příloha č. 3: Modelový příklad aktivních prvků

Seznam použitých switchů PROV sítě

určení	počet	typ
core switch	2 ks	Core_SW
access switch 48 port PoE	19 ks	SW_Typ_1
access switch 48 port	14 ks	SW_Typ_2
access switch AV režie	1 ks	SW_Typ_3
access switch optický	1 ks	SW_Typ_4

Umístění switchů PROV sítě v uzlových bodech a využití portů

	odhadované minimální využití portů PROV sítě									
	různé provozní VLAN									
Místnost	provozní	Digital sig.	WiFi	Gastro	celkem	instalované	ks	1 switch	ks	2. a další switch
MDF.1a	0	12	2	0	**16**	2	1	SW_Typ_1		-
MDF.1b							1	SW_Typ_4		
IDF.-1.1	15	8	6	4	**29**	134	1	SW_Typ_1		-
IDF.-1.2	47	8	8	0	**64**	123	1	SW_Typ_1	1	SW_Typ_2
IDF.-1.3	20	0	4	0	**24**		1	SW_Typ_1		-
MDF.2	22	0	0	0	**22**	27	1	SW_Typ_1		-
AV patch MP	0	0	0	0	**0**			-		-
IDF.1.1	47	18	13	4	**84**	130	1	SW_Typ_1	1	SW_Typ_2
IDF.1.2	56	19	15	8	**98**	162	1	SW_Typ_1	2	SW_Typ_2
IDF.1.3	40	18	14	4	**77**	143	1	SW_Typ_1	1	SW_Typ_2
IDF.1.4	41	24	14	4	**84**	140	1	SW_Typ_1	1	SW_Typ_2
IDF.3.1	60	29	11	5	**105**	238	1	SW_Typ_1	2	SW_Typ_2
IDF.3.2	30	29	11	4	**74**	187	1	SW_Typ_1	1	SW_Typ_2
IDF.3.3	44	0	4	0	**48**	144	1	SW_Typ_1		-
IDF.4.1	44	0	4	0	**48**	133	1	SW_Typ_1	1	SW_Typ_2
IDF.5.1	15	21	10	12	**62**	140	1	SW_Typ_1	1	SW_Typ_2
IDF.5.2	6	21	10	12	**49**	113	1	SW_Typ_1	1	SW_Typ_2
IDF.5.3	7	21	10	7	**45**	108	1	SW_Typ_1	1	SW_Typ_2
IDF.5.4	8	21	10	9	**48**	113	1	SW_Typ_1	1	SW_Typ_2
IDF.6.1	10	0	6	0	**16**	50	1	SW_Typ_3		-
IDF.6.2	0	0	0	0	**0**			-		-
IDF.6.3 (press)	44	0	4	0	**48**	142	1	SW_Typ_1		-
IDF.7.1	0	0	36	0	**36**		1	SW_Typ_1		-
PROV.CORE1							1	Core_SW		
PROV.CORE2							1	Core_SW		

SFP transceivery pro PROV-ozní síť

Následující modelová tabulka obsahuje seznam všech SFP transceiverů pro potřeby sítě PROV vč. rezerv a dále také malé množství SFP transceiverů pro provozní a diagnostické účely. Tabulka jako taková je modelová (počty nejsou závazné) a skutečné počty a typy dodá Zhotovitel dle jím navrženého a realizovaného řešení.
Navíc Zhotovitel dodá jako rezervní SFP BiDi transcievery v počtu 8 párů (16 ks) typu, které Zhotovitel používá pro propojení mezi Core Switchem a Access switchem. Zhotovitel může využít polovinu z rezervních SFP BiDi transcieverů jako okamžitě dostupnou rezervu skladem na Arena Brno. Druhá polovina může být použita pro jiné potřeby Objednatele.

Seznam SFP transceiverů pro PROV

určení	popis	Počet ks
Strana CORE	10G SFP+ LC BiDi 40km-D 1330/1270 XCVR (R9X54A)	42 (+8)
Strana access	10G SFP+ LC BiDi 40km-U 1270/1330 XCVR (R9X55A)	42 (+8)
Strana CORE	25G SFP28 BiDi 1330/1270	4
Strana access	25G SFP28 BiDi 1270/1330	4
Strana access	1G SFP LC BiDi 1310/1550	20
Strana prvek	1G SFP LC BiDi 1550/1310	20
Stacking	10G SFP+ DAC, Direct Attach Copper Cable (J9281D), 1m	26
Core propojky	25G SFP28 DAC, Direct Attach Copper Cable, 1m	4 (2+2)
Operativní provozní	10Gb SFP+ RJ45 metalický transciever	4
Operativní provozní	1G SFP RJ45 metalický transciever	8

Příloha 4: Schémata

Schéma PROV-ozní sítě (aktivní prvky)

viz dále

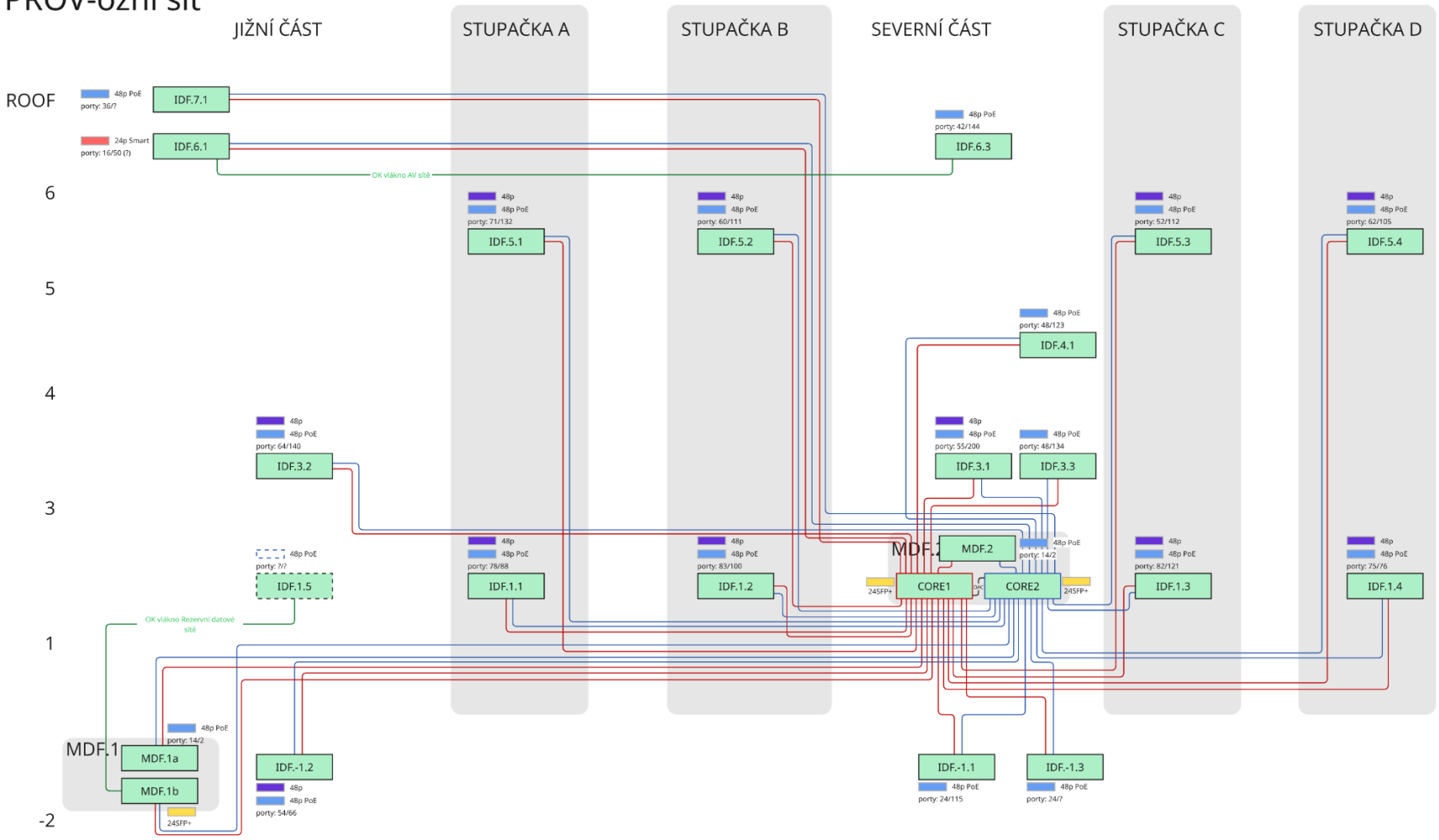
Schéma optické kabeláže Základní datové sítě

viz dále

Příloha 5: Půdorysy MDF a IDF

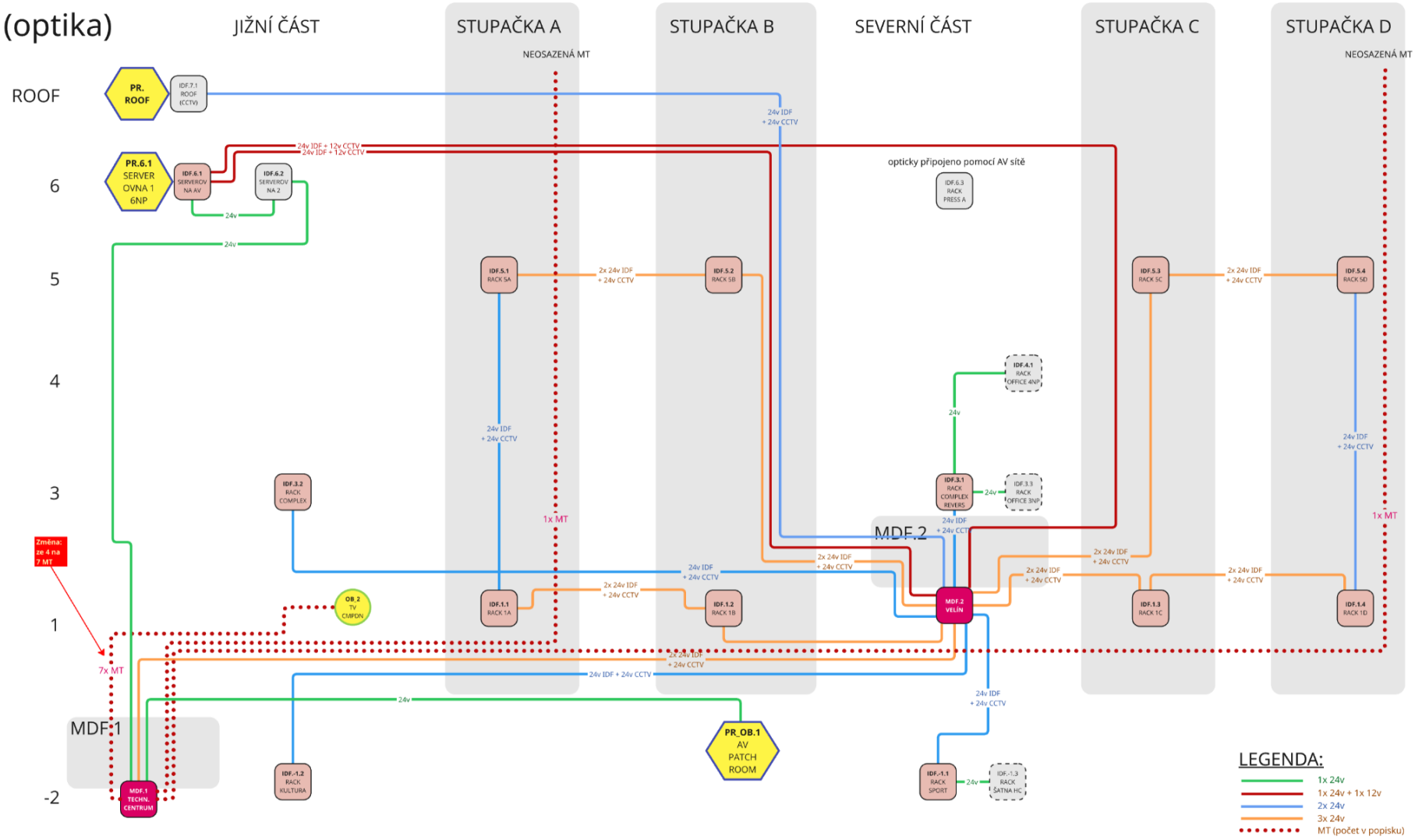
(samostatný dokument)

PROV-ozní síť



Pozn: Uzly sítě (MDF a IDF) jsou v grafice doplněny barevnými boxíky, které reprezentují použité switche. U boxíku je stručně typ switche, barva boxíku odpovídá barvě v tabulce aktivních prvků. U boxíku je i odhad využití portů: <minimálně využito>/<instalováno>
Boxíky vyznačené čárkovaně nejsou součástí dodávky (jde o výhled).

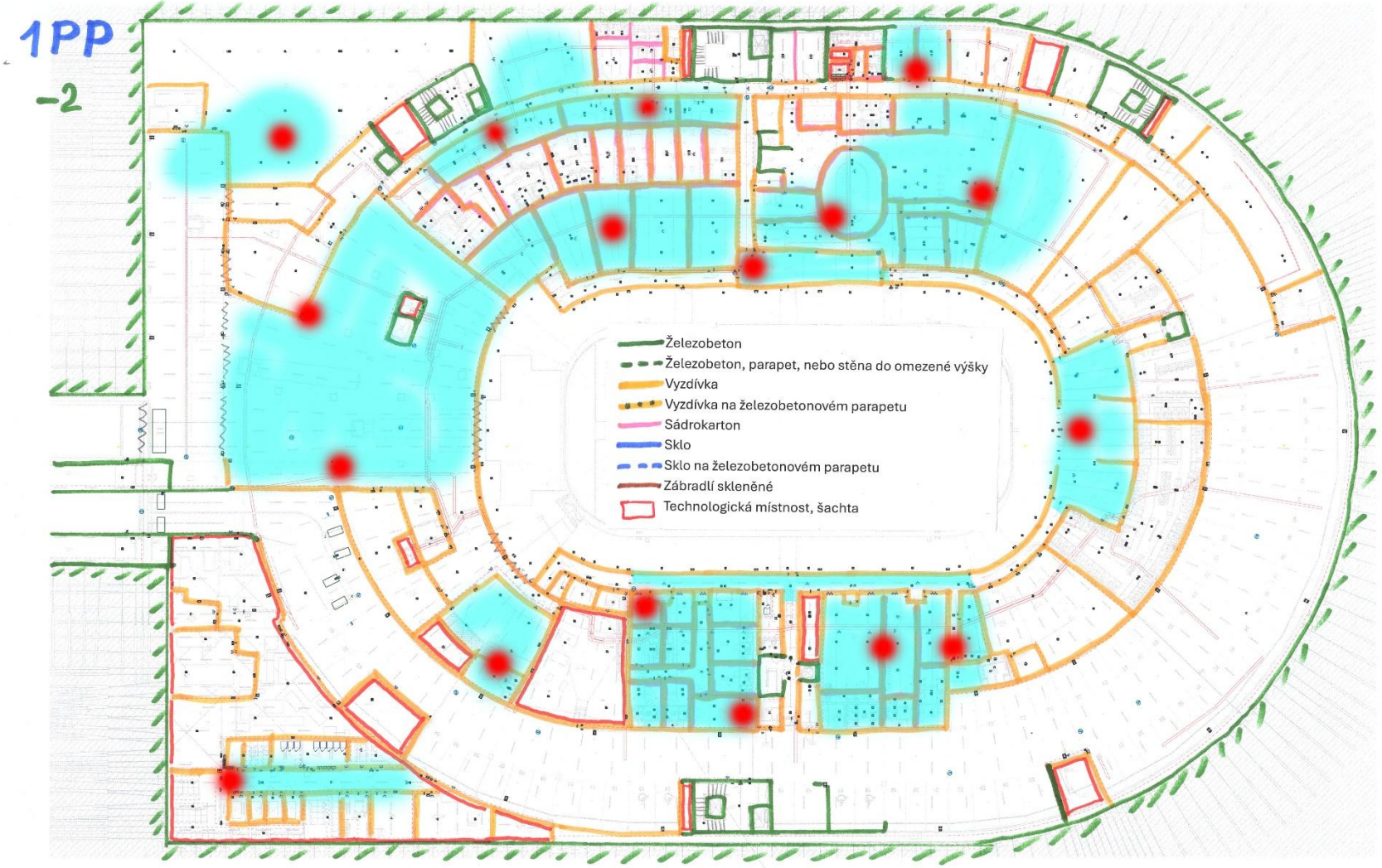
Základní datová síť (optika)

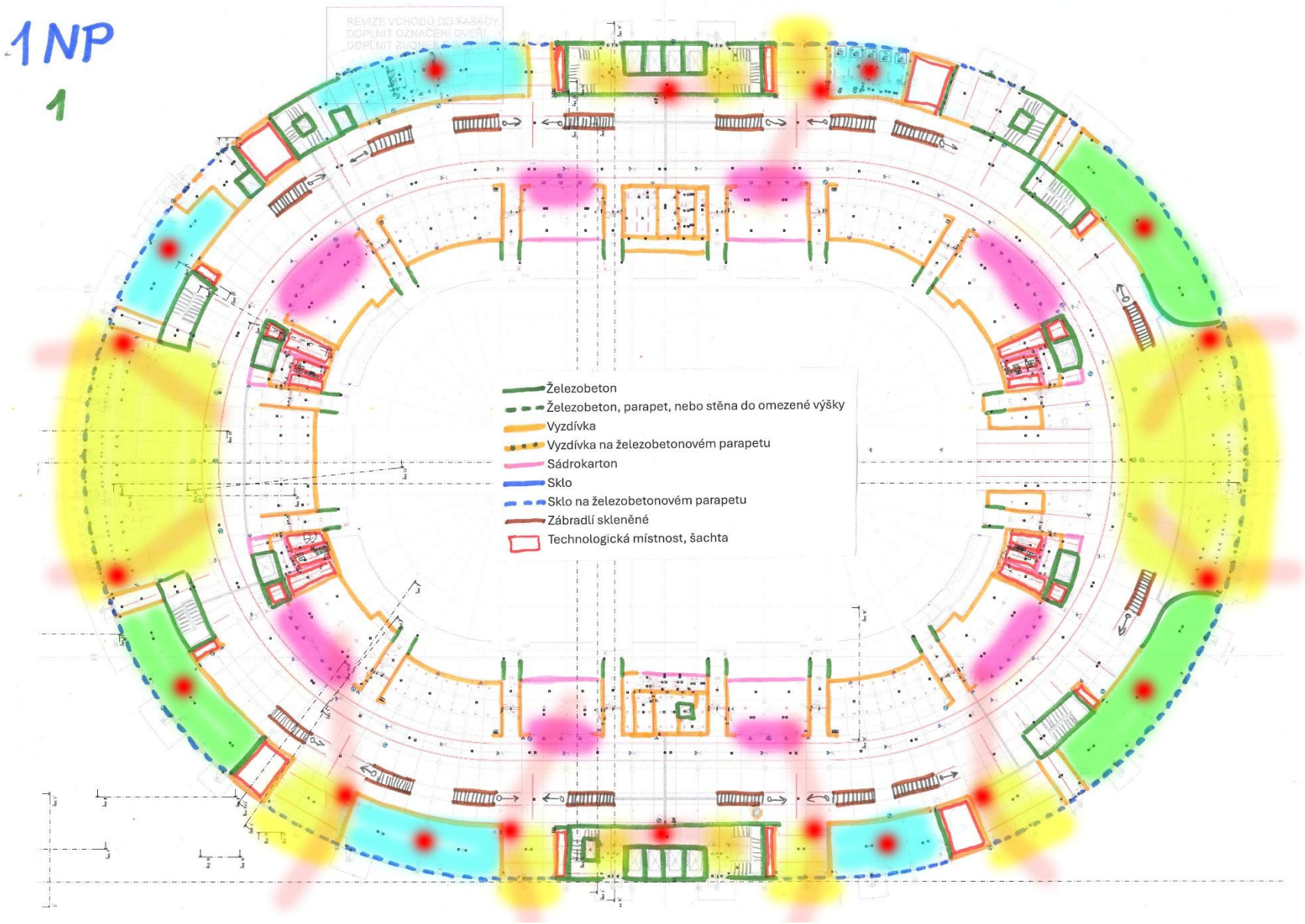


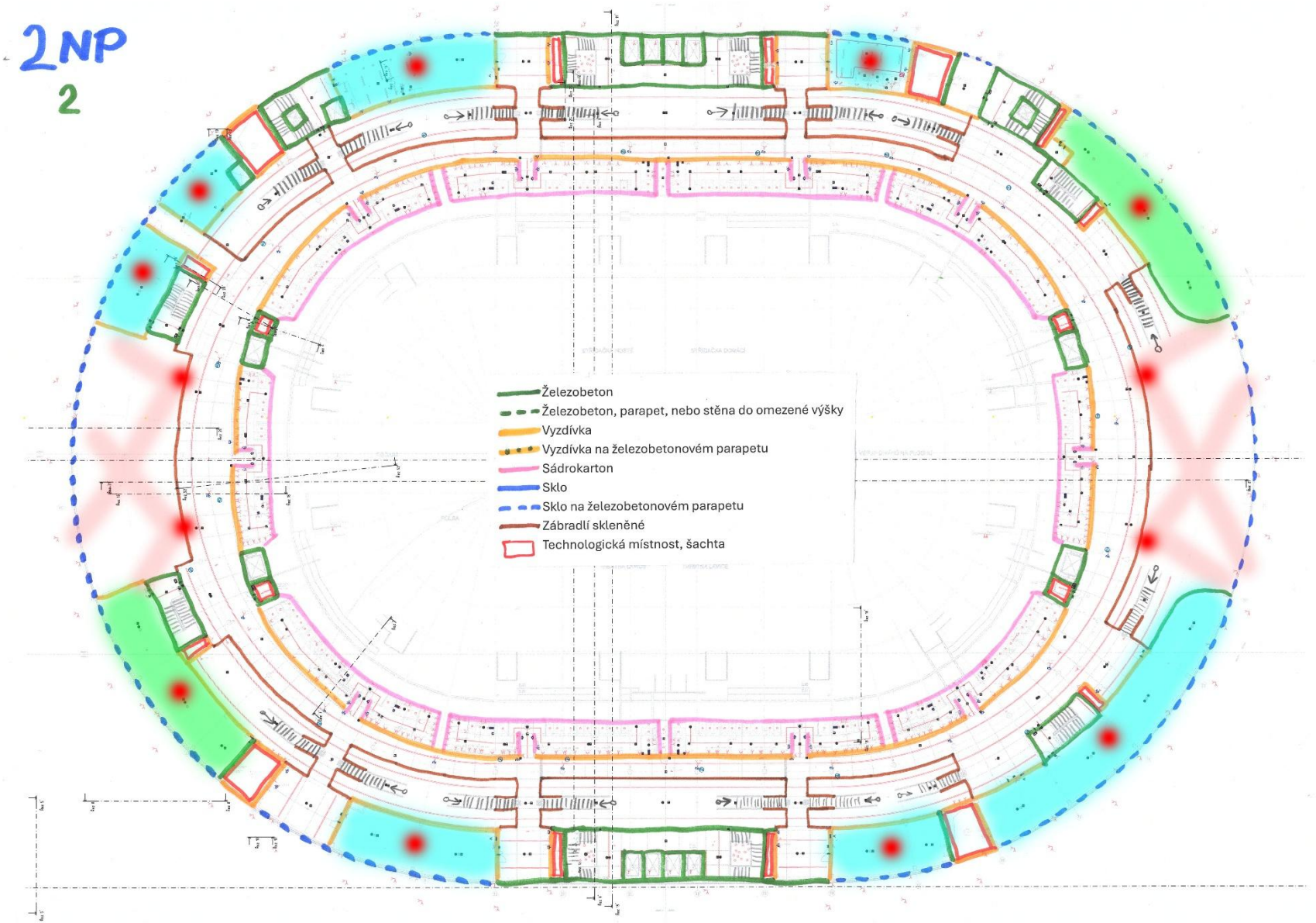
Pozn: Červenou poznámkou je zvýrazněna změna oproti předchozí definici Základní datové sítě.

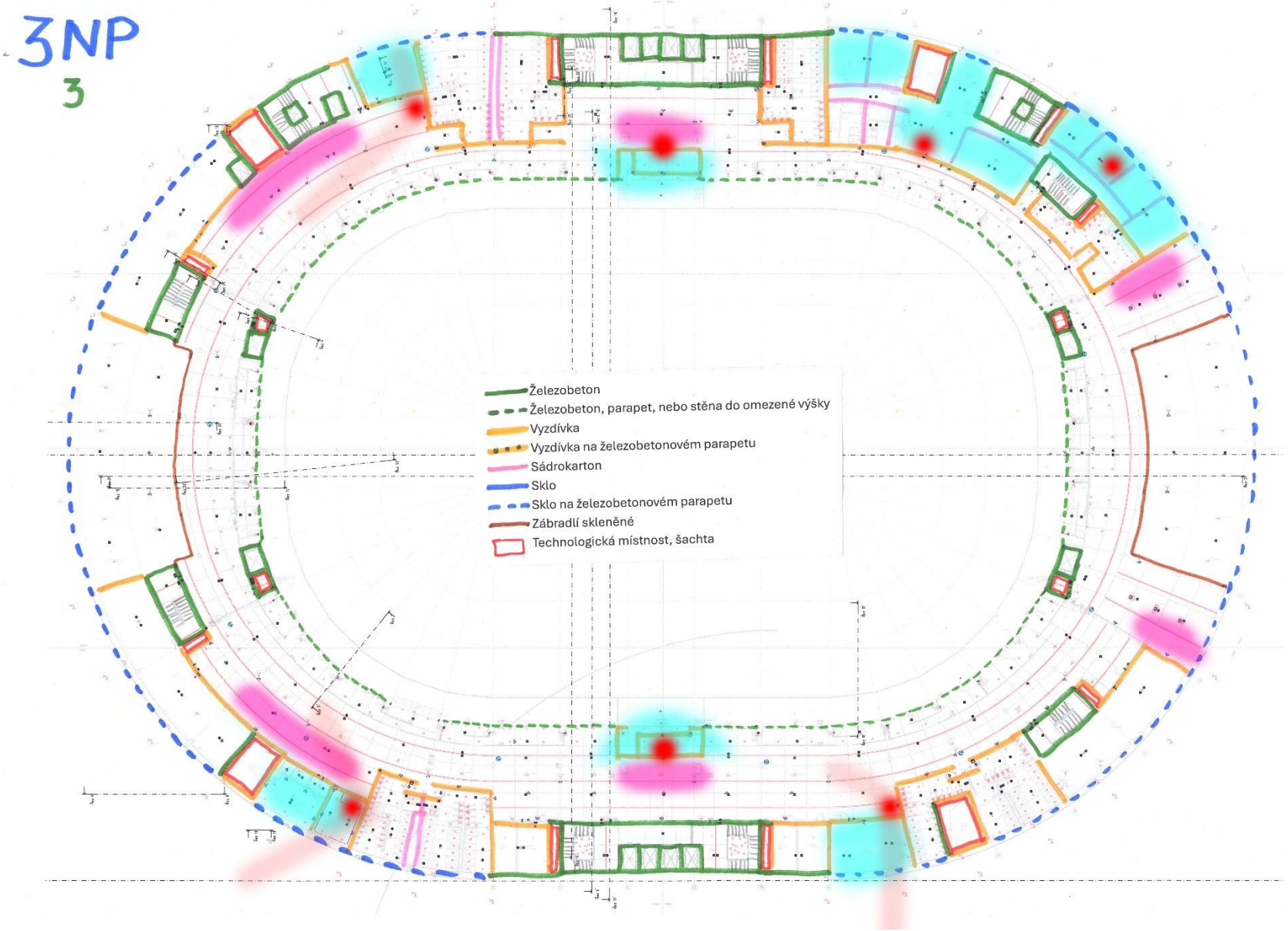
Příloha 6: Modelové umístění WiFi AP

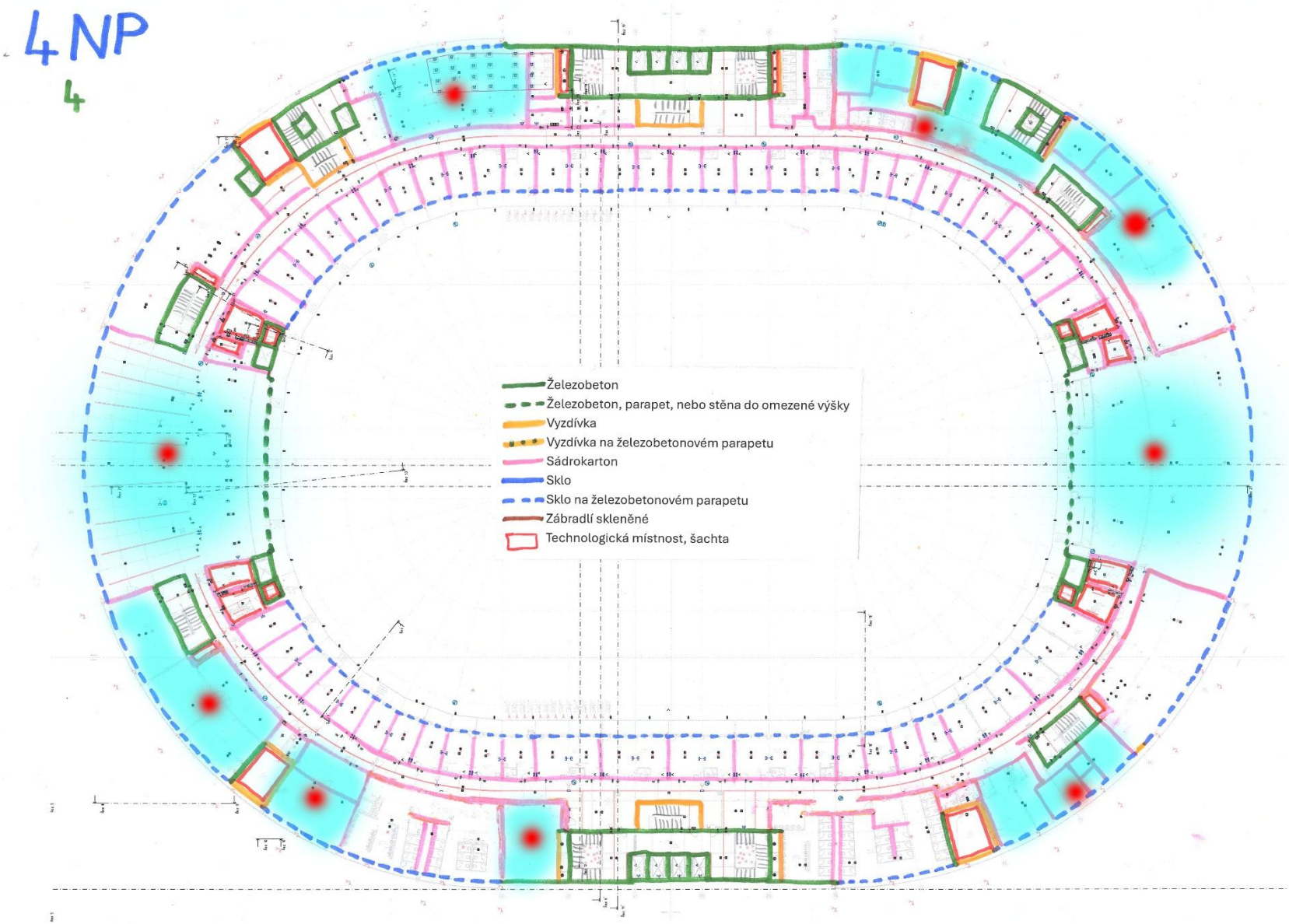
Na půdorysech jsou červenými značkami znázorněny přibližné modelové umístění WiFi AP dle předběžného návrhu investora. Z nich vyplývá předpokládaný stropový počet WiFi AP pro nabídkovou cenu.

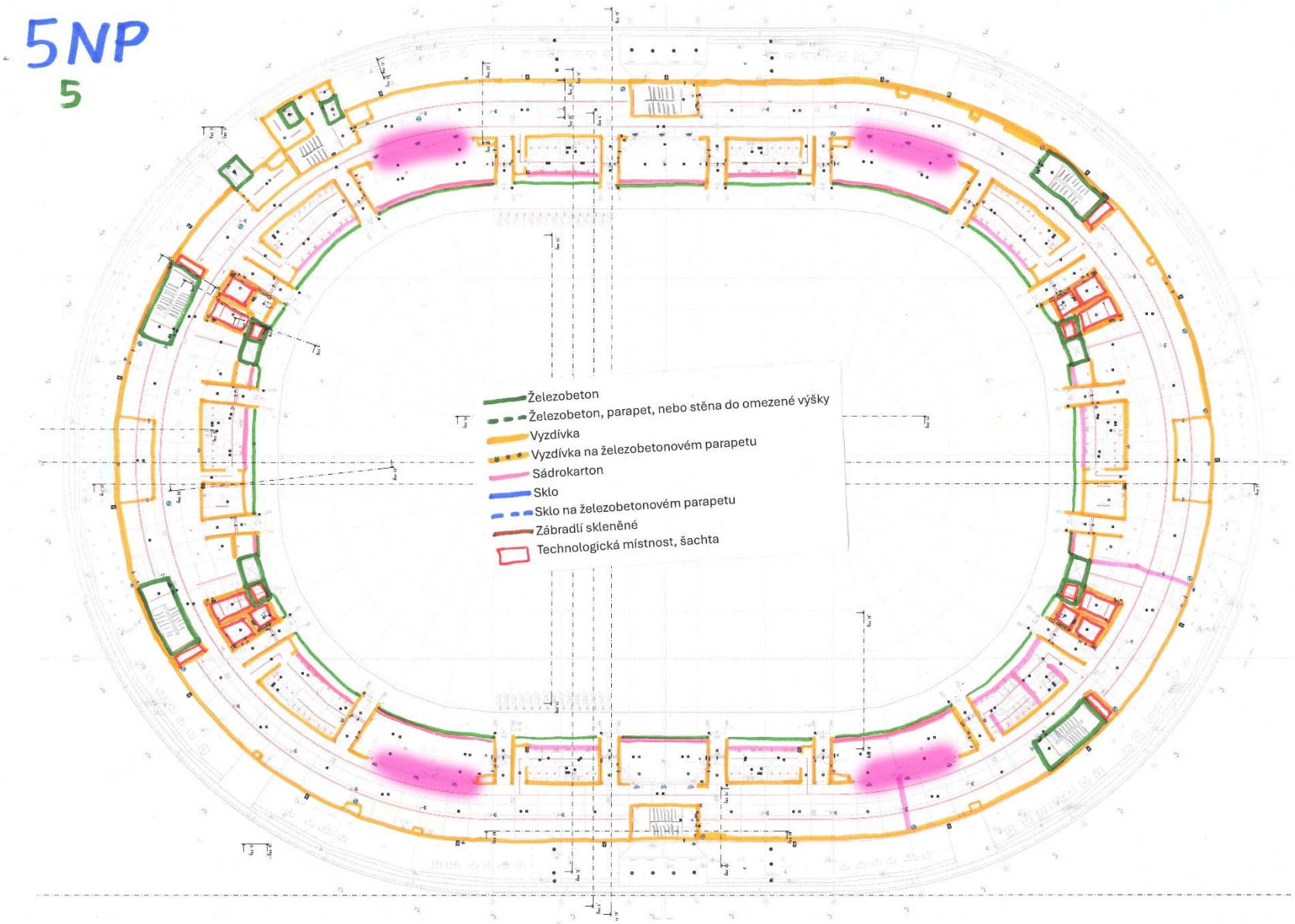

1PP
-2
Železobeton
Železobeton, parapet, nebo stěna do omezené výšky
Vyzdívka
Vyzdívka na železobetonovém parapetu
Sádrokarton
Sklo
Sklo na železobetonovém parapetu
Zábradlí skleněné
Technologická místnost, šachta


1 NP
1
Železobeton
Železobeton, parapet, nebo stěna do omezené výšky
Vyzdívka
Vyzdívka na železobetonovém parapetu
Sádrokarton
Sklo
Sklo na železobetonovém parapetu
Zábradlí skleněné
Technologická místnost, šachta


2 NP
2
Železobeton
Železobeton, parapet, nebo stěna do omezené výšky
Vyzdívka
Vyzdívka na železobetonovém parapetu
Sádrokarton
Sklo
Sklo na železobetonovém parapetu
Zábradlí skleněné
Technologická místnost, šachta

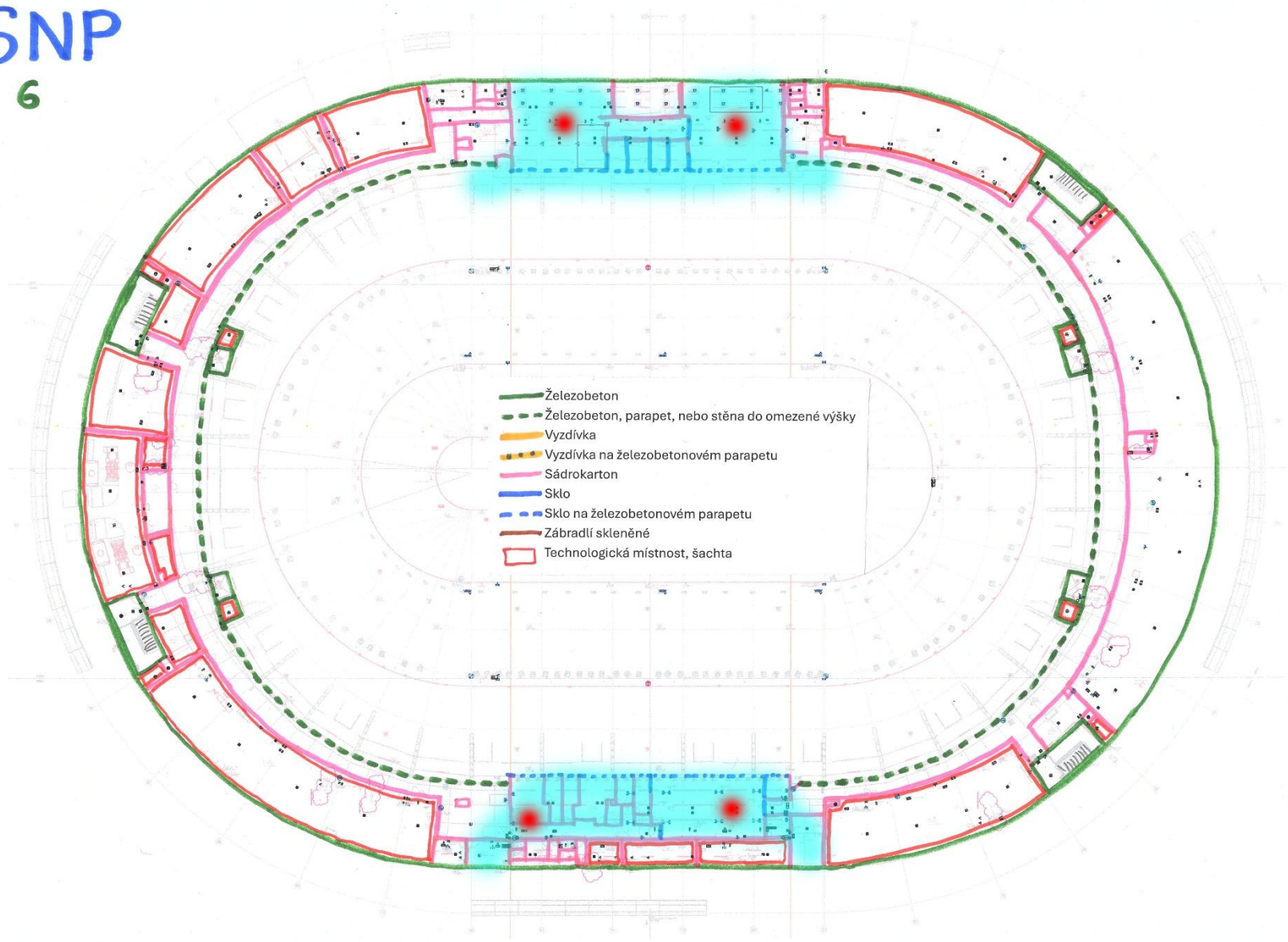

3NP
3
Železobeton
Železobeton, parapet, nebo stěna do omezené výšky
Vyzdívka
Vyzdívka na železobetonovém parapetu
Sádrokarton
Sklo
Sklo na železobetonovém parapetu
Zábradlí skleněné
Technologická místnost, šachta


4 NP
4
Železobeton
Železobeton, parapet, nebo stěna do omezené výšky
Vyzdívka
Vyzdívka na železobetonovém parapetu
Sádrokarton
Sklo
Sklo na železobetonovém parapetu
Zábradlí skleněné
Technologická místnost, šachta


5NP
5
Železobeton
Železobeton, parapet, nebo stěna do omezené výšky
Vyzdívka
Vyzdívka na železobetonovém parapetu
Sádrokarton
Sklo
Sklo na železobetonovém parapetu
Zábradlí skleněné
Technologická místnost, šachta

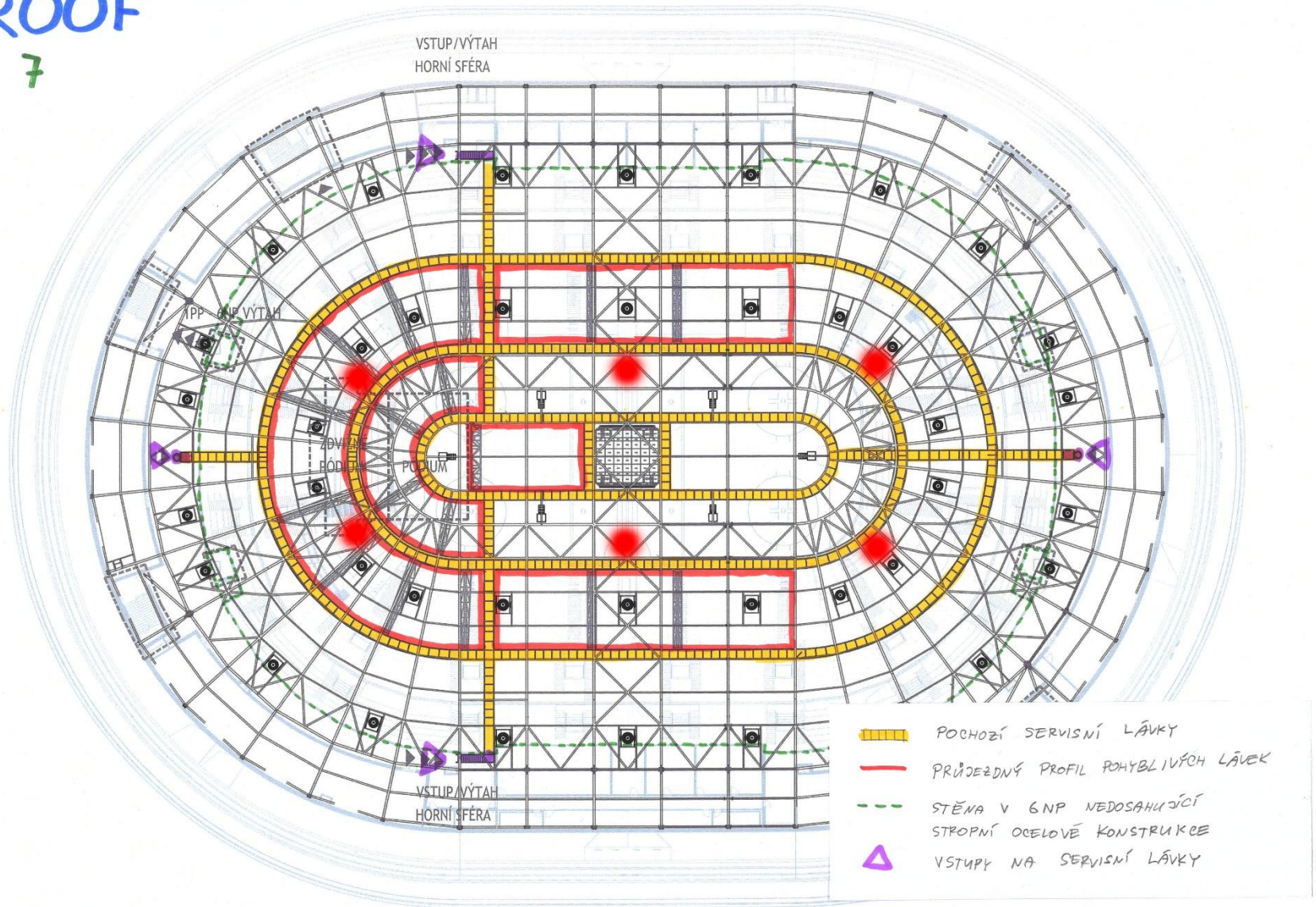
6NP

6


Železobeton
Železobeton, parapet, nebo stěna do omezené výšky
Vyzdívka
Vyzdívka na železobetonovém parapetu
Sádrokarton
Sklo
Sklo na železobetonovém parapetu
Zábradlí skleněné
Technologická místnost, šachta

ROOF

7


VSTUP/VÝTAH
HORNÍ SFÉRA
PODIUM
VSTUP/VÝTAH
HORNÍ SFÉRA
POCHOZÍ SERVISNÍ LÁVKY
PRŮJEZDNÝ PROFIL POHYBLIVÝCH LÁVEK
STĚNA V 6NP NEDOSAHUJÍCÍ STROPNÍ OCELOVÉ KONSTRUKCE
VSTUPY NA SERVISNÍ LÁVKY

9. Seznam kritických náhradních zařízení

Virtualizace:

- 1ks záložní disk pro diskové pole (shodný s dodaným vystrojením diskového pole) - (skladem na ARENA BRNO) nebo je alternativně možné dodat diskové pole se 2 osazenými spare disky
    - slouží k okamžitému servisu na místě, bude vyhrazena jen jako rezerva k okamžitému nasazení

Provozní datová síť ARENA BRNO:

- 1x IDF switch 48port PoE univerzálně naprogramovaný (skladem na ARENA BRNO)
    - Objednatel upřesňuje pojem "univerzálně naprogramovaný"
        - Jedná se o konfiguraci switche tak, aby obsahoval na určených portech určené VLAN bez dalších speciálních parametrů. Např. 4x VLAN po 12 portech. Konkrétní zadání dodá Objednatel během instalace, správa switche v dalším čase bude shodná se správou zbylých aktivních prků PROVozní sítě
    - slouží jako okamžitá náhrada nefunkčních zařízení i když mohou být v danou chvíli Objednatelem využita na jiném místě budovy v místě s nízkou prioritou a Zhotovitel může toto zařízení ihned použít k okamžitému servisu
- 1x switch s min 2x SFP28 (nebo rychlejšími) a min. 20x SFP+ (nebo rychlejší), k němu odpovídající BiDi transceivery
    - konkrétní modely a počty SFP transcieverů určí Zhotovitel na základě jeho návrhu propojení s Core switchi - jedná se o BiDi transcievery na linkách k Core Switchům
    - slouží jako okamžitá náhrada nefunkčních zařízení i když může být v danou chvíli Objednatelem využita na jiném místě budovy v místě s nízkou prioritou a Zhotovitel může toto zařízení ihned použít k okamžitému servisu
- 12 ks SFP RJ45-1GBit a 8 ks SFP+ RJ45-10GBit a 4 páry (8 ks) BiDi transceiverů SFP+10Gbit
- slouží jako náhradní a servisní zařízení výhradně pro potřebu Zadavatele (vše skladem na ARENA BRNO)

WiFi:

- 5x WiFi AP nejběžnějšího typu (skladem na ARENA BRNO)
- 1x WiFi AP každého dalšího použitého typu (skladem na ARENA BRNO)
- Všechny výše uvedené položky WiFi slouží jako okamžitá náhrada nefunkčních zařízení i když mohou být v danou chvíli Objednatelem využita na jiném místě budovy v místě s nízkou prioritou a Zhotovitel může toto zařízení ihned použít k okamžitému servisu

10. ICT provozní uživatelské scénáře

Provozní datová síť

Uživatel (odborně proškolený pracovník AB / osoba s odpovídající odbornou kvalifikací - dále jako “uživatel”) musí být s využitím Zhotovitelem dodaných SW nástrojů s GUI rozhraním (tam, kde je to možné) schopen těchto provozních změn a reakcí na vzniklé provozní potřeby a stavy:

- vytvoření/odstranění VLAN, změna parametrů (routing mezi VLAN, připojení do internetu), např. pro přivedení VPN služeb z MDF.0 na daný port v budově
- přidělování VLAN na porty access switchů, vč. taggovaných (trunk) VLAN
- propojení s VLAN v jiné fyzické síti (např. s AV sítí)
- řízení rychlosti ve VLAN, nastavit QoS priorit pro VLANy, případně prioritizace konkrétních IP
- spravovat Spanning tree protokol pro ochranu před smyčkami (per VLAN, např. RSTP, PVST...)
- zablokovat typ provozu (TCP, UDP na konkrétním portu)
- nastavit PortSecurity (MAC) na konkrétních portech, na některých naopak bez
- nastavení rychlosti konektivity do internetu (nebo další parametry) pro konkrétní NAT zónu nebo VLAN
- měnit přidělované rozsahy adres na DHCP serveru, rezervovat IP adresy, přidávat podsítě s DHCP v nových VLAN apod.
- nastavit několik NAT (na různých veřejných IP)
    - různé varianty kombinací která VLAN je ve které NAT skupině (zóně)
    - port forwarding, DMZ
- nastavit firewallu ve vztahu k použití několika veřejných IP
- Spravovat nastavení load balancingu mezi více ISP a automatického failover:
    - Load balancing mezi primárním a sekundárním ISP (rovnoměrné rozložení provozu)
    - Automatický failover na záložního ISP (mikrovlna) s "nouzovým" režimem - přepnutí QoS profilu na routeru a firewallu (omezení šířky pásma, prioritizace kritického provozu)
    - V provozu lze mít nastavenou buď variantu load balancingu (primární + sekundární ISP), nebo variantu failover (jeden aktivní ISP + záložní mikrovlna)

    - **Zhotovitel dodá řešení, které umožní technicky realizovat load balancing mezi dvěma ISP a současně zajistí failover na terciární ISP (mikrovlna) s automatickým přepnutím QoS profilu. Toto přepnutí proběhne v případě výpadku hlavního ISP a výpadkem se myslí ztráta konektivity do internetu.**
- nastavit IPSec tunely (a jiné VPN technologie)
- nastavit na firewallu připojení routeru promotéra na veřejnou IP
- zařadit switche promotéra do topologie PROV sítě, typicky pro eSport event:
    - Objednatel upřesňuje: Např. na volném portu Core SW nebo optickém portu AccesSW uživatelsky nastavit trunk. Do daného portu bude připojen další (rozšiřující) AccesSwitch ve správě Objednatele nebo promotéra.
- spravovat DHCPguard na Access SW

Uživatel dále prostřednictvím nástrojů dodaných Zhotovitelem

- má možnost provádění základního monitoringu sítě (DHCP list, stav propojovacích linek mezi aktivními prvky atd.)
- má možnost sledovat vytížení sítě jako celku, v uzlových bodech (Access SW…) a na konkrétních portech (AP…) a dokáže tak získat informace pro sběr zkušeností z provozu

WiFi síť ARENA BRNO

Uživatel musí být s využitím Zhotovitelem dodaných SW nástrojů s GUI rozhraním (tam, kde je to možné) schopen těchto provozních změn a reakcí na vzniklé provozní potřeby a stavy:

- vytvořit další SSID
- změnit parametry SSID (beacon, name, hidden…)
- změnit zabezpečení SSID (free, radius server (přes IDM), nebo klasické WPA pswd, nastavení šifrování…)
- změnit parametry pokrytí (přiřazení SSID konkrétním AP, změna kmitočtu, kanálu, šířky kanálu)
- přidat další AP operativně do sítě (posílení pokrytí v daném místě, vytvoření jednoúčelové SSID v konkrétním místě)
- spravovat přiřazení konkrétních SSID do konkrétních VLAN