**Příloha č. 3 ZD – Požadavky na vyhotovení Realizace pokrytí**

Veřejná zakázka: „Vybudování zabezpečené WIFI sítě“

Dodavatel:………….., IČO: …………………. *(Pozn.: Doplní dodavatel, poté poznámku vymaže.)*

**Příloha č. 1 Smlouvy o dílo – Požadavky na vyhotovení Realizace pokrytí**

# Obecné požadavky

Předmětem plnění veřejné zakázky je dodávka, instalace, konfigurace prvků bezdrátové sítě včetně dodání do místa plnění, zaškolení obsluhy a zajištění záručního servisu a podpory.

Součástí plnění je dodávka veškerého instalačního materiálu, optické, metalické a napájecí propojovací kabely a moduly, včetně dodávek potřebných materiálů a zařízení nezbytných pro řádné dokončení předmětu plnění a zajištění jeho provozuschopnosti. Součástí dodávky a instalace s konfigurací jsou všechny licence potřebné pro provoz a management celkového dodaného počtu všech prvků bezdrátové sítě. Nabízené technické řešení musí být plně kompatibilní se stávající počítačovou sítí Zadavatele.

Součástí plnění je úklid a odvoz všech obalů a dalších materiálů používaných při vlastní instalaci v souladu s ustanoveními zákona 185/2001 Sb., o odpadech, ve znění pozdějších předpisů z místa plnění.

Dodavatel je povinen v rámci plnění veřejné zakázky garantovat nabízené technické parametry a doložit přesné označení nabízeného produktu včetně jeho technických parametrů pro ověření splnění požadavků Zadavatele.

Předmět plnění veřejné zakázky bude prováděn dle platných právních předpisů ČR a obecně závazných vyhlášek platných v místě realizace veřejné zakázky, dle ČSN EN a technických norem souvisejících s předmětem plnění.

Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství). Zboží musí být určeno pro český trh. Zadavatel požaduje potvrzení výrobce, že se jedná o zboží pro český trh. Zadavatel bude v DB výrobce uveden jako první vlastník.

Z důvodu požadavku na jednotný management bezdrátové sítě budou kontroléry a Access Pointy pocházet od jednoho výrobce.

Účastník je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení), že jsou určeny pro český trh.

Je požadována záruka na hardware kontroléru s výměnou NBD v délce min. 60 měsíců a záruka na hardware ostatních komponent v délce min. 36 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.

# Popis stávajícího stavu

Stávající bezdrátová síť je složena z řídících prvků a bezdrátových přístupových bodů různých výrobců. Jednotlivé přístupové body jsou propojeny pomocí metalické kabeláže v interní síti, která je postavena na přepínačích CISCO:

* Cisco Catalyst 2960
* Cisco Catalyst 2950
* Cisco Catalyst 3560
* Cisco Catalyst 3750
* Cisco Catalyst 3850

Jednotlivé areály jsou propojeny optickými kabely a tvoří jednu interní síť.

Budovy jsou umístěny v areálech DOPRAVNÍHO PODNIKU OSTRAVA a.s.:

1. budova ředitelství, Poděbradova 494/2, Moravská Ostrava, 702 00 Ostrava;
2. areál tramvaje Moravská Ostrava, Plynární 3345/20, Moravská Ostrava, 702 00 Ostrava;
3. areál tramvaje Poruba, U Vozovny 1115/3, 708 00 Ostrava – Poruba;
4. areál trolejbusy Ostrava, Sokolská 3243/64, Moravská Ostrava, 702 00 Ostrava;
5. areál autobusy Hranečník, Počáteční 1962/36, Slezská Ostrava, 710 00 Ostrava;
6. areál autobusy Poruba, Slavíkova 6229/27A, 708 00 Ostrava – Poruba;
7. areál dílny Martinov, Martinovská 3293/40, 723 00 Ostrava – Martinov.

# Požadované technické parametry zařízení

## Wifi access point

### Wifi access point vnitřní

| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované funkcionality**  **Ano/NE** | **Bližší specifikace (Označení, typ, atd.)** |
| --- | --- | --- |
| Třída zařízení - Vnitřní AP |  |  |
| Typ antén interní |  |  |
| Access Point vybavený radiem pro 2,4 a 5 GHz pásmo, podpora standardu 802.11a/b/g/n/ac wave 2 |  |  |
| Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz |  |  |
| Podpora minimálně 3x3 MIMO, MU-MIMO a až 80 MHz kanál pro 802.11ac w2 |  |  |
| Minimální počet inzerovaných SSID (BSSID) per radio 8 |  |  |
| 1x 10/100/1000 Ethernet rozhraní |  |  |
| Nastavitelný DTIM interval (Delivery Traffic Indication Message) pro jednotlivé WLAN |  |  |
| Mapování SSID do různých VLAN podle IEEE 802.1Q |  |  |
| Přenosová rychlost v pásmu 5 GHz min. 867 Mbps |  |  |
| Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli nebo přes IPv4 a IPv6 pomocí Telnet nebo SSH |  |  |
| Možnost napájení z 802.3af nebo at PoE injectoru |  |  |
| Vypínatelné indikační LED diody informující o stavu zařízení |  |  |
| Pracovní režim AP řízené kontrolérem (lightweight) |  |  |
| Access Point určený pro instalaci na strop/podhled, součástí je montážní příslušenství |  |  |

### Wifi access point speciální

| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované funkcionality**  **Ano/NE** | **Bližší specifikace (Označení, typ, atd.)** |
| --- | --- | --- |
| Třída zařízení - Vnitřní AP |  |  |
| AP uzavřené konstrukce, bez větracích otvorů a ventilátoru |  |  |
| Typ antén interní pro obě pásma |  |  |
| Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2 |  |  |
| Podpora standardů 802.11a/b/g/n a 802.11ac wave 2 |  |  |
| Podpora 4x4 MIMO, podpora MU-MIMO, až 160 MHz kanál pro 802.11ac |  |  |
| Minimální počet inzerovaných SSID (BSSID) per radio 8 |  |  |
| Dvě rádia pracující v režimu 2,4 a 5 GHz pro standardní prostředí nebo duální 5 GHz pro HD nasazení, možnost provozovat AP v monitorovacím režimu |  |  |
| Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark) |  |  |
| Podpora standardů IEEE 802.3af (PoE) a IEEE 802.3at (PoE+) |  |  |
| 2x 10/100/1000 Ethernet rozhraní |  |  |
| Hardware filtry pro filtraci intermodulačního rušením pocházejícím z mobilních sítí (Advanced Cellular Coexistence nebo obdobné) |  |  |
| Vypínatelné indikační LED diody informující o stavu zařízení |  |  |
| Band Steering či obdobné (prioritizace 5GHz pásma v případě je-li podporováno) |  |  |
| Mapování SSID do různých VLAN podle IEEE 802.1Q |  |  |
| Podpora spektrální analýzy v pásmech 2,4GHz a 5GHz (detekce zdroje rušivého signálu – interference) |  |  |
| Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli nebo přes IPv4 a IPv6 pomocí Telnet nebo SSH |  |  |
| Napájení AP pomocí PoE dle standardu 802.3at bez nutnosti redukce výkonu 5GHz rádia |  |  |
| Access Point určený pro instalaci na strop/podhled, součástí je montážní příslušenství |  |  |

### Wifi access point 802.11ax

| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované funkcionality**  **Ano/NE** | **Bližší specifikace (Označení, typ, atd.)** |
| --- | --- | --- |
| Třída zařízení - Vnitřní AP |  |  |
| AP uzavřené konstrukce, bez větracích otvorů a ventilátoru |  |  |
| Typ antén intení |  |  |
| Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2 |  |  |
| Podpora standardů 802.11a/b/g/n a 802.11ac wave 2 |  |  |
| Certifikace dle standardu IEEE 802.11ax - Wi-Fi CERTIFIED 6. |  |  |
| Podpora 4x4 MIMO, podpora MU-MIMO, až 160 MHz kanál pro 802.11ac |  |  |
| Dvě rádia pracující v režimu 2,4 a 5 GHz pro standardní prostředí nebo duální 5 GHz pro HD nasazení, možnost statické i dynamické volby režimu, možnost provozovat AP v monitorovacím režimu |  |  |
| Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark) |  |  |
| Podpora standardů IEEE 802.3af (PoE) a IEEE 802.3at (PoE+) |  |  |
| 2x 10/100/1000 Ethernet rozhraní |  |  |
| Vypínatelné indikační LED diody informující o stavu zařízení |  |  |
| Band Steering či obdobné (prioritizace 5GHz pásma v případě je-li podporováno) |  |  |
| Mapování SSID do různých VLAN podle IEEE 802.1Q |  |  |
| Podpora spektrální analýzy v pásmech 2,4GHz a 5GHz |  |  |
| Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 a IPv6 pomocí Telnet a SSH |  |  |

### Wifi access point přenosný

| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované funkcionality**  **Ano/NE** | **Bližší specifikace (Označení, typ, atd.)** |
| --- | --- | --- |
| Třída zařízení: indoor přístupový bod-kompaktní |  |  |
| Uzavřená konstrukce bez ventilátorů |  |  |
| Access Point vybavený radiem pro 2,4 a 5 GHz pásmo, podpora standardu 802.11a/b/g/n/ac wave 2 |  |  |
| Pracovní režim AP bez kontroléru (autonomní) |  |  |
| Pracovní režim AP řízené kontrolérem (lightweight) |  |  |
| USB port s podporou 3G/4G USB modemu jako WAN uplink |  |  |
| Mapování SSID do různých VLAN podle IEEE 802.1Q |  |  |
| DHCP server, směrování a NAT pro bezdrátové klienty |  |  |
| AP v režimu IPSec VPN klient s možností tvorby L2 či L3 VPN |  |  |
| CLI formou serial konsole port |  |  |
| Minimální počet portů ethernet LAN: 4x 100/1000 Mbit/s RJ45 |  |  |
| Podpora napájení z AC napájecího zdroje |  |  |
| Podpora spektrální analýzy v pásmech 2,4GHz a 5GHz (detekce zdroje rušivého signálu – interference) |  |  |

## Wifi access point venkovní

| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované funkcionality**  **Ano/NE** | **Bližší specifikace (Označení, typ, atd.)** |
| --- | --- | --- |
| Třída zařízení - Venkovní AP |  |  |
| Vestavěná interní MIMO anténa omni všesměrová |  |  |
| Access Point vybavený radiem pro 2,4 a 5 GHz pásmo, podpora standardu 802.11a/b/g/n/ac wave 2 |  |  |
| Podpora MIMO a počet nezávislých streamů 2x2:2, až 80 MHz kanál pro 802.11ac |  |  |
| Certifikace dle standardu IEEE 802.11ax - Wi-Fi CERTIFIED 6. |  |  |
| Přenosová rychlost v pásmu 5 GHz min. 867 Mbps |  |  |
| Minimální počet inzerovaných SSID (BSSID) per radio 8 |  |  |
| Venkovní provedení s krytím IP67, rozsah provozních teplot -40° až +55°C |  |  |
| 1x 10/100/1000 Ethernet rozhraní |  |  |
| Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli nebo přes IPv4 a IPv6 pomocí Telnet nebo SSH |  |  |
| Podpora spektrální analýzy v pásmech 2,4GHz a 5GHz (detekce zdroje rušivého signálu – interference) |  |  |
| Možnost napájení z 802.3af nebo at PoE injectoru |  |  |
| Vypínatelné indikační LED diody informující o stavu zařízení |  |  |
| Mapování SSID do různých VLAN podle IEEE 802.1Q |  |  |
| Pracovní režim AP řízené kontrolérem (lightweight) |  |  |
| Součástí AP je příslušenství pro montáž |  |  |

# Wifi controller

| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované funkcionality**  **Ano/NE** | **Bližší specifikace (Označení, typ, atd.)** |
| --- | --- | --- |
| Požadovaný formát zařízení: Fyzické zařízení - nepřipouští se virtulizovaný kontrolér |  |  |
| Počet optických portů 10Gbit/s s volitelným fyzickým rozhraním: 4x 10Gbit/s SFP+ |  |  |
| Podorovaný počet AP bez nutnosti přidávání hardware: 512 AP |  |  |
| Podpora Redundance (HA) kontrolerů v režimech: active-active a active-standby. |  |  |
| Výpadek aktivního kontroleru v redundantním páru nemá dopad na provoz již připojených klientů (tj. bez potřeby opětovné autentizace) |  |  |
| Možnost redundantního napájecího zdroje |  |  |
| Podporovaný počet současně připojených klientů: min. 16000 |  |  |
| Tunelování uživatelských dat z AP až na kontrolér, možnost šifrování těchto dat |  |  |
| Vzdálené lokality - možnost lokálního bridgování uživatelských dat per SSID přímo na příslušném AP |  |  |
| Aplikační inspekce přenášeného provozu (DPI na 7. vrstvě ISO/OSI na základě aplikačních signatur) umožňující rozpoznání jednotlivých aplikací, grafické zobrazení statistik a možnost řízení QoS per rozpoznaná aplikace |  |  |
| Podpora pro 802.11u, 802.11v a 802.11k |  |  |
| RJ45 konzolový port a/nebo USB konzolový port |  |  |
| Podpora wireless MESH s protokolem pro výběr optimální cesty a podporovanou hloubkou min. 8 hopů, automatický výběr vhodného kanálu pro backhaul, současné připojení normálních a mesh AP k jednomu kontroléru |  |  |
| Podpora rozpoznávání aplikací na 7. vrstvě |  |  |
| WPA3, WPA/WPA2-PSK, WPA/WPA2-Enterprise, 802.1X, MAC autentizace |  |  |
| Vestavěný “captive portal” pro návštěvníky s podporou nativních IPv6 klientů, s možností úpravy vzhledu a přidáním vlastního loga, včetně vestavěného rozhraní pro vytváření dočasných guest účtů s možností definice jejich platnosti |  |  |
| Podpora linkové agregace IEEE 802.3ad |  |  |
| Podpora správy přes serial CLI nebo přes IP pomocí SSH/telnet a https web GUI, SNMP |  |  |
| Grafický uživatelský dashboard zobrazujicí kvalitu a obsazenost kanálů, jednotlivé klienty |  |  |
| Funkce řízení a ochrany rádioveho spektra s automatickou optimalizací sítě (přidělováni kanálů, fast roaming, rozdělení klientů na jednotlivá AP) |  |  |
| Podpora spektrální analýzy |  |  |
| Podpora standardu „802.11w“ pro ochranu řídících rámců na AP a klientovi |  |  |
| Podpora API rozhraní pro plnou konfiguraci kontroléru |  |  |
| Podpora Rogue Wireless detekce a containment |  |  |
| Podpora VLAN podle IEEE 802.1Q (VLAN 4000) |  |  |
| Podporované autentizační/autorizační zdroje: RADIUS, LDAP, RFC 3576 Change of Authorization |  |  |
| Plná kompatibilita s nabízenými přístupovými body |  |  |
| Sdílení licencí mezi více kontroléry |  |  |
| Automatické dynamické rozpoznání a prioritizace hlasových protokolů jako SIP, SCCP, VOCERA a SVP pomocí funkce DPI |  |  |
| Integrovaný Wireless IPS s podporou wireless containment, možnost vynuceného odpojení klientů od cizích AP |  |  |

# SW řešení pro řízení přístupu

| **Požadované funkcionalita/vlastnost** | **Způsob splnění požadované funkcionality/vlastnosti**  **ANO/NE** | **Bližší specifikace (Označení, typ, atd.)** |
| --- | --- | --- |
| On premise řešení pro externí captive portál pro zaměstnance DPO a návštěvy a jejich rozšířenou autentizaci (pro min. 400 hostů) |  |  |
| Appliance musí být od stejného výrobce jako kontroler bez nutnosti dodatečných licencí např. pro OS nebo databáze |  |  |
| Podpora 802.1X autentizace pro bezdrátové sítě, Ethernet LAN sítě a VPN |  |  |
| Možnost vytváření clusterů více virtuálních instancí. Cluster pak musí poskytovat vysokou dostupnost pro všechny funkcionality řešení a zároveň možnost navýšení počtu podporovaných uživatelů přidáním další instance. Cluster bude podporovat active-active režim pro ověřování |  |  |
| Podpora RADIUS CoA podle RFC3576 |  |  |
| Platforma podporuje změnu autorizačního stavu zařízení bez nutnosti změny definice autorizační politiky, např. pro odpojení nebo karanténu koncových zařízení |  |  |
| Podpora minimálně následujících metod autentizace: PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace |  |  |
| Podpora TACACS+ autentizace správců síťových zařízen |  |  |
| Možnost využití autentizace a autorizace min: LDAP, MS AD, Token, MAC auth, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta) |  |  |
| Podpora autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, osobní profil či skupina v Active Directory |  |  |
| Možnost integrace s MDM (Mobile Device Management) platformami třetích stran (minimálně AirWatch, Citrix, MobileIron) |  |  |
| Podpora REST API |  |  |
| Podpora REST volání vyvolaného autentizační či autorizační událostí (minimálně pro předání informací o klientovi jinému systému, automatického založení support ticketu atp.) |  |  |
| Zpracovávání syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Minimálně v rozsahu přijmutí bezpečnostního hlášení z firewallu a izolace konkrétního klienta na základě tohoto hlášení. |  |  |
| Administrátor systému musí mít možnost vlastní tvorby parseru/integrace syslog hlášení pro možnost uživatelské integrace s libovolnými systémy třetích stran. |  |  |
| Sběr dodatečných informací o připojených zařízeních (“profiling”) jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace musí být možné využít pro doplňkové ověření přístupu zařízení do sítě. |  |  |
| Možnost registrace zařízení pomocí MAC adresy pro non-IT uživatele - omezená funkce administračního rozhraní, se zařazením zařízení do skupiny s definovanou politikou přístupu. |  |  |
| Podpora autentizace pomocí účtů sociálních sítí – Google, Google Plus, Facebook, Facebook WIFI, Twitter, LinkedIn, Microsoft |  |  |
| Podpora autentizace lokálními účty v rámci portálu, ověření pomocí jméno+heslo, autentizační kód |  |  |
| Možnost samoobslužné registrace hosta do sítě s SMS a email ověřením |  |  |
| Možnost přístupu zdarma pouze s akceptací podmínek užití |  |  |
| Možnost vynucení odpojení zařízení ihned po naplnění jakéhokoliv z limitů |  |  |
| Perzistence autentizace/registrace skrze MAC caching a zobrazení už jen uvítacích stránek s osobním oslovením hosta při dalších návštěvách |  |  |
| Možnost provozovat více graficky i obsahově unikátních portálů v rámci jedné instalace |  |  |
| SW maintenance a technická podpora poskytnutá výrobcem na 3 roky |  |  |

# Příslušenství

Napájení přístupových bodů bude realizováno pomocí 16-ti multiportových PoE injektorů velikost 1U, umístěných v datových rozvaděčích, které musí být kompatibilní s dodávanými AP.