# Integrovaná územní strategie Ostravské metropolitní oblasti 2021-2027

**Vymezení podporovaného projektu v SC 4.1 IROP 2021-2027 v oblasti zájmového vzdělávání**

**Zdůvodnění:**

**V programovém období 2021-2027 je potřeba se zaměřit na zavedení moderních vyučovacích metod do vyučování v základních školách, ale i v zájmovém vzdělávání. V rámci území ostravské metropolitní oblasti je zjištěna potřeba kvalitního vzdělávání přírodovědných předmětů, digitálních kompetencí, technického vzdělávání a výuky cizích jazyků. Účelem Strategie ITI ostravské metropolitní oblasti 2021-2027 je tedy zvýšit zájem o výuku samotných předmětů, ale i kvalitně připravit žáky základních škol na střední školy všeobecného a technického zaměření, respektive na případné vysokoškolské studium přírodních a technických věd tak, aby byli schopni obstát ve zvyšujícím se konkurenčním prostředí. Komunikace nebo alespoň orientace v minimálně jednom cizím jazyku je v současné době nezbytností. Vše je propojeno digitálními technologiemi, proto je na výuku informatiky (práce s digitálními technologiemi) kladen nemenší důraz. Zájmové vzdělávání má v procesu vzdělávání důležitou úlohu a spolu s formálním vzděláváním je jednou ze zásadních cest, jak docílit výše uvedeného kýženého zlepšení, které je žádoucí hlavně v oblasti výuky konceptu STEM, (Science – přírodní vědy) (Technology – technologie), (Engineering – technika) a (Mathematics – matematika). Napomoci má zavedení virtuální (VR), rozšířené (AR) a mixované (MR), případně prodloužené/rozšířené reality (XR) do výuky výše zmíněných klíčových kompetencí. Další cestou je využití umělé inteligence. Toto vše ke zefektivnění výuky (efektivní metody předávání informací, zlepšení soustředění na probírané téma, zábavnější forma vzdělávání). Veškerá technika pracuje na základě internetového připojení, proto dobře fungující konektivita je neméně důležitá.**

Společné téma:

# POKROČILÉ METODY VE VZDĚLÁVÁNÍ

**Aktivity:**

Pořízení vybavení odborných učeben (multimediálních) pokročilými výukovými pomůckami s důrazem na zapojení robotů (humanoidů), virtuální reality (VR), rozšířené reality (AR) a mixované reality (MR) do výuky přírodních věd, techniky a práce s digitálními technologiemi, případně propojení předmětů v rámci těchto klíčových kompetencí. Může se jednat i o mobilní učebny.

**Klíčové kompetence (KK):**

- přírodní vědy,
- technické obory,
- práce s digitálními technologiemi.

**Vybavení:**

**HARDWARE**

(PC, notebooky, tablety, VR brýle, MR brýle, roboti (humanoidi), mobilní telefony, jejich příslušenství apod.)

**SOFTWARE**

(k ovládání pořizovaného hardware, specializované softwary pro výuku konkrétních předmětů, programy pro interaktivní výuku, 3D modely apod.)

**NÁBYTEK**

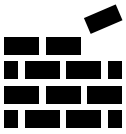
(pořízení nábytku a vybavení laboratoří, dílen, odborných a specializovaných učeben, výukových prostor)

**KONEKTIVITA**

V rámci strategického projektu bude řešena i konektivitu v alespoň minimálním standardu konektivity základních škol (pokud už ve škole není vyřešeno). V rámci projektu není ale možné realizovat pouze aktivitu na zajištění vnitřní konektivity.

**STAVEBNÍ ÚPRAVY**

Stavby, stavební úpravy a modernizace odborných a specializovaných učeben a výukových prostor ve vazbě na aktivity tohoto strategického projektu.



**BEZBARIÉROVOST**

Pokud v době realizace projektu není odborná učebna nebo budova bezbariérově dostupná, musí být v projektu řešena. Výdaje na bezbariérovost ale nebudou oprávněnými výdaji projektu.

**OBECNÉ USTANOVENÍ**

V rámci Strategie ITI ostravské metropolitní oblasti je třeba realizovat projekty, které efektivně skloubí investici do vzdělávací infrastruktury s inovativním a efektivním způsobem vzdělávání. Tzn. bude podpořen takový projekt, který počítá se zapojením všech žáků v rámci jednoho kroužku - bude pořízeno dostatečné množství vybavení pro zapojení všech žáků v rámci kroužku, zájmové aktivita apod.

Příklad: Kapacita učebny 10 míst/žáků - učebna bude vybavena 10 ks VR brýlí nebo adekvátním počtem laboratorních soustav nebo měřících zařízení, apod.

**CÍLOVÉ SKUPINY**

- žáci
- pedagogičtí pracovníci

**OPRÁVNĚNÍ ŽADATELÉ**

- zřizovatelé vzdělávacích zařízení (obce, městské obvody, městské části)
- církevní školy

**SPECIÁLNÍ PODMÍNKY**

Množství předložených projektových záměrů (PZ) je omezeno. Každý žadatel může předložit pouze 1 PZ. V případě, že je zřizovatelem obec nebo jiný subjekt, který je zřizovatelem více vzdělávacích zařízení (středisek, domů dětí a mládeže), bude předkladatelem projektového záměru na strategický projekt zřizovatel a předloží projekt, ve kterém řeší více (všechny) zařízení.

## STANDARD KONEKTIVITY

(definováno a převzato z IROP)

**Parametry konektivity jsou relevantní pouze v případě, když v rámci projektu v IROP je tato aktivita realizována. Současný stav konektivity ve škole není hodnocen.**

Povinným výstupem projektu je zapracování zásad využívání ICT a přístupu k síti do vnitřních předpisů školy, v případě že je tato aktivita realizována v rámci projektu IROP.

### 1. Konektivita školy k veřejnému internetu (WAN)

**Obecný popis:** pro základní způsobilost projektu naplňujícího opatření „vnitřní konektivita škol“ musí příslušná škola zajistit kvalitní připojení ke službám veřejného internetu a to i v případě, že vybavení pro připojení k internetu není předmětem projektové žádosti. Za toto připojení je považováno zajištění konektivity splňující následující minimální parametry v době ukončení realizace projektu:

- šíře pásma (bandwidth) odpovídající 128kbps/student[1] nebo 512kbps/počítač[2] nebo taková šířka pásma, která neomezuje provoz zařízení a uživatelů[3]

[1] *Počet studentů je definovaný celkový počet studentů školy*

[2] *Metrika vhodná typicky pro školy bez mobilních popř. BYOD zařízení*

[3] *Definováno jako saturace šířky pásma připojení k veřejnému internetu, která ani ve špičkách nedosáhne a to ani krátkodobě 100%*

  - vlastní nebo poskytovatelem přidělené veřejné IPv4 i IPv6 adresy
  - plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack)
- validující DNSSEC resolver na straně školy
- podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení
- logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)
- síťové zařízení podporující rate limiting, antispoofing, ACL/xACL, rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality
- zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu, antivirovou kontrolou stahovaného obsahu
- možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků
- podpora DNSSEC a IPv6 protokolů pro služby školy dostupné online
- u software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po celou dobu udržitelnosti projektu.

Nad rámec těchto povinných parametrů je dále doporučeno v rámci projektu realizovat:

- symetrické připojení bez agregace a omezení (FUP)
- zapojení poskytovatele připojení v bezpečnostním projektu FENIX resp. veřejné adresy využívané školou jsou zapojeny do infrastruktury FENIX[4] nebo ISP splňuje alespoň technické standardy definované projektem FENIX – viz http://nix.cz/cs/file/NIX_PRAVIDLA_FENIX

## 2. Vnitřní konektivita školy (LAN)

**Obecný popis:** vnitřní síťové prostředí školy pořizované v rámci projektu může být řešeno pevnou sítí, bezdrátovou sítí, nebo kombinací těchto síťových technologií. Připojením je nutné pokrýt prostory dotčené hlavním projektem, rovněž je možné pokrýt ostatní prostory školy, včetně chodeb, jídelen, internátu a dalších školských zařízení. Potřebnost a účelnost takového pokrytí musí být zdůvodněna ve studii proveditelnosti.

Povinné minimální bezpečnostní parametry projektu (bez ohledu typ síťového připojení):

- Monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) - RFC3954 nebo ekvivalent (např. NetFlow) – systém pro monitorování a sběr provozně-lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN) a to bez negativních vlivů na zátěž a propustnost zařízeni s kapacitou pro uchování dat po dobu minimálně 2 měsíců
- Povinné řešení systému správy uživatelů (Identity Management), tj. centrální databáze identit (LDAP, AD, apod.) a její využití pro autentizaci uživatelů (žáci i učitelé) za účelem bezpečného a auditovatelného přístupu k síti, resp. síťovým službám.
- logování přístupu uživatelů do sítě umožňující dohledání vazeb *IP adresa – čas – uživatel*

*[4] V případě, kdy má ISP přidělené IP adresy od člena FENIX, musí být součástí projektu prohlášení ISP, ze kterého bude patrné, že příslušné adresy jsou v rámci FENIX propagovány. V případě, kdy má ISP vlastní ASn a není přímý člen FENIX, musí být součástí projektu prohlášení ISP, ze kterého bude patrné, že příslušné ASn propaguje do FENIX na základě smluvního vztahu některý ze členů FENIX.*

V oblasti pevné LAN musí projekt splňovat následující minimální parametry:

- Minimální konektivita stanic a dalších koncových zařízení zařízení 100Mbit/s fullduplex
- Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP,…)
- Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1Gbit/s fullduplex
- Páteřní rozvody mezi budovami v areálu realizovány prostřednictvím optických, metalických vláken popř. bezdrátovými spoji v licencovaném pásmu (povolení ČTÚ)
- Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3)[5] s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,…

V případě řešení bezdrátových sítí (wifi) pak musí projekt naplňovat následující minimální parametry:

- Podpora mechanismu izolace klientů
- Návrh topologie wifi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou ve v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů
- Centralizovaná architektura správy wifi sítě (centrální řadič, centrální management, tzv. thin access pointy, popř. alespoň centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravované access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení)
- Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD …)
- Podpora standardu IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz
- Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu

Nad rámec těchto povinných parametrů je dále doporučeno v rámci projektu realizovat:

- Minimálně pasivní zapojení[6] do federovaného systému eduroam (www.eduroam.cz). Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů.

## 3. Další bezpečnostní prvky

**Obecný popis:** v rámci projektů je možné realizovat další aktivity naplňující principy bezpečného využívání IT prostředků. Zejména pak jde o:

- Identity management systémy (IDM) – systém správy identit, řízení životního cyklu uživatelů, integrace do provozních a bezpečnostních systémů
- Centralizovaný autentizační systém napojení na systém správy identit (např. na bázi LDAP, AD, studijní a personální agendy apod.)
- Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty, blokace wifi v určitém čase)

---

[5] *Požadavek se týká prvků, přes které je veden veškerý provoz, resp. jde o centrální prvky. Podružné přepínače (chodbové, učebnové) musí splňovat pouze požadavek na neblokující architekturou přepínacího subsystému*

[6] *Pasivním zapojením se rozumí poskytování služeb sítě eduroam na úrovni poskytovatele zdrojů – viz. http://www.eduroam.cz/_media/cs/cz_roam_policy_v2.0.pdf*

- Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací a zpřístupnění jejich služeb)
- Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3954 nebo ekvivalent (NetFlow))
- Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie
- Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management)
- Systémy pro monitorování funkčnosti síťové a serverové infrastruktury (např. Nagios/Icinga)
- Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk)
- Nástroje pro centrální správu a audit ICT prostředků
- Systémy zálohování a obnovy dat serverové infrastruktury
- Systémy pro antivirovou ochranu zařízení, antispamovou ochranu poštovních serverů
- Zabezpečení přístupových protokolů (SSL/TLS) služeb (např. emailové služby, webové servery, studijní a ekonomické agendy) atp.
- Podpora vzdáleného přístupu (VPN)