Příloha č. 1 výzvy Zásad pro poskytování finančních příspěvků na zvyšování IT vybavení organizací zřizovaných Krajem Vysočina v roce 2020

Tento dokument definuje základní okruhy podpory včetně technických kritérií cílového stavu infrastruktury organizace a přijatelnosti výdajů a aktivit projektů v rámci Zásad pro poskytování finančních příspěvků na zvyšování IT vybavení organizací zřizovaných Krajem Vysočina:

1. Konektivita organizace k veřejnému internetu a dalším WAN sítím
2. Vnitřní konektivita organizace (LAN)
3. Bezpečnost
4. Software
5. Virtualizace
6. Specifické IT/technické vybavení organizace

Cílem podpory této výzvy Zásad je příspěvek zřizovatele na pořízení vybavení (SW i HW) pro pokrytí specifických potřeb hlavní činnosti příspěvkové organizace Kraje Vysočina. Typicky jde o vybavení, které je specifické pro chod organizace, ale jehož pořízení může být problematické z pohledu standardního finančního plánu organizace. Jde např. o pořízení technického řešení, které je jednorázové, nepravidelné, nečekané a nejde o prostou obnovu stávajícího vybavení, případně jde o nový produkt/technologie na trhu nebo nezbytnou reakci na změnu podmínek popř. legislativy.

**Konektivita organizace k veřejnému internetu a dalším WAN sítím**

Cílem je zajištění vysokorychlostního, bezpečného a stabilního připojení organizace k veřejnému internetu a dalším WAN sítím (neveřejným) s důrazem na využití sítí a služeb poskytovaných krajem (ROWANet, Cesnet, síťové služby TCK). Připojení organizace by mělo podporovat moderní technické standardy (IPv6 resp. dual-stack), identifikaci a autentizaci uživatelů (proxy, RADIUS, logování NAT, NAC), bezpečné publikování online služeb, ochrana před kybernetickými útoky (firewall, emailové brány, antivirové filtry). Konektivita musí být o dostatečné kapacitě.

**Způsobilé výdaje**:

* síťové zařízení WAN-LAN (router, firewall, NAT; s podporou přepínání/směrování protokolů IPv4/IPv6 a minimální propustností přepínacího/směrovacího subsystému 1 Gbps),
* bezpečnostní zařízení (IDS, IPS, aplikační firewall, NAC),
* nezbytné vybavení a vedení poslední míle k přípojnému bodu poskytovatele internetu nebo sítě ROWANet popř. propojení budov organizace (rádiový přijímač, anténní zařízení, metalické nebo optické vedení na pozemku a v budovách organizace),
* nezbytné licence SW a nákup HW související s funkcionalitou síťového nebo bezpečnostního zařízení (např. síťové rozhraní atp.) rozhraním WAN-LAN včetně funkcionality možnosti vzdálené správy a monitoringu funkčnosti zařízení (ICMP echo, SNMP v3, HTTPS, SSH apod.),
* nezbytné vybavení pro umístění, instalaci a provoz technologie (např. rack, napájení, UPS/přepěťová ochrana, kabeláž, chlazení atp.) a zajištění DMZ zóny pro síťové a serverové technologie, včetně rezervy/možnosti rozšíření navrhovaného řešení.

**Nezpůsobilé výdaje**: zřizovací a provozní náklady na zajištění připojení (konektivity) organizace, náklady na licenční poplatky ČTÚ, služby údržby aktivních prvků a bezpečnostních zařízení s výjimkou standardní záruky, povinné servisní poplatky, maintenance a podpora nově pořizovaného SW/HW na více než 1 rok, maintenance a podpora dříve pořízeného SW/HW.

**Vnitřní konektivita organizace (LAN)**

Cílem aktivit v rámci této části výzvy je zajištění vnitřního síťového prostředí organizace a to prostřednictvím pevné sítě, bezdrátové sítě, nebo kombinací těchto síťových technologií.

Řešení pořízené v rámci projektu musí respektovat standardní bezpečnostní parametry (bez ohledu na typ síťového připojení), a to včetně monitorování IP datových toků formou exportu detailních provozních informací o přenesených datech, řešení systému správy uživatelů (Identity Management) a její využití pro autentizaci uživatelů přistupujících k síti a logování přístupu uživatelů do sítě umožňující dohledání vazeb *IP adresa – čas – uživatel.* V případě pevné LAN musí projekt splňovat zejména požadavek minimální konektivity 100 Mbps fullduplex, a dále by měl zahrnovat strukturovanou kabeláž pro připojení stanic a zařízení, zajištění páteřních rozvodů mezi budovami optickým vláknem, včetně aktivních prvků s neblokující architekturou přepínacího subsystému(wirespeed) podpora 802.1Q VLAN, podpora 802.1X, RADIUS based MAC autentizace.

V případě řešení bezdrátových sítí (Wi-Fi), pokud je projekt řeší, požadujeme popis návrhu topologie Wi-Fi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou v příslušných prostorách organizace a s kapacitami pro provoz mobilních zařízení.

Současně pak musí projekt naplňovat následující minimální parametry:

* Podpora mechanismu izolace klientů.
* Centralizovaná architektura správy Wi-Fi 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.
* V případě školských zařízení minimálně pasivní zapojení[[1]](#footnote-2) do federovaného systému eduroam ([www.eduroam.cz](http://www.eduroam.cz)). Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů.
* Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu.

**Způsobilé výdaje**:

* aktivní prvky, servery, síťové sondy a analyzátory,
* strukturovaná kabeláž pro připojení koncových zařízení,
* páteřní rozvody optickým vláknem
* Wi-Fi vysílače, systém centrálního řízení Wi-Fi (centrální řadiče),
* úložiště pro kolektory,
* SW nezbytný pro provoz infrastruktury (licence OS, přístupové licence), standardní záruka.

**Nezpůsobilé výdaje**: počítačové stanice, realizace poskytnutí formou služby (X as a service) kromě služeb přímo souvisejících s dodávkou a implementací HW a SW; cloudové služby (např. cloud management) způsobilé jen v investiční fázi projektu, služby údržby aktivních prvků a bezpečnostních zařízení s výjimkou standardní záruky, pozáruční servis, rozšířená záruka.

**Bezpečnost**

V rámci projektů zaměřených na bezpečnost je možné realizovat aktivity naplňující standardní principy bezpečného využívání IT prostředků.

**Způsobilé výdaje** aktivit v rámci projektů řešících bezpečnost zahrnují SW, HW, licence, náklady na implementaci a integraci přímo související s pořizovaným SW a HW, pokud se jedná o následující:

* Identity management systémy (IDM) – systém správy identit, řízení životního cyklu uživatelů, integrace do provozních a bezpečnostních systémů a to včetně integrace na IDM kraje.
* Síťový firewall.
* Proxy včetně možnosti kategorizace webových stránek.
* Centralizovaný autentizační systém napojení na systém správy identit (např. na bázi LDAP, AD, studijní a personální agendy apod.).
* Zapojení do autentizační federace kraje VysocinaID - <https://vysocinaid.kr-vysocina.cz/>.
* Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty, blokace wifi v určitém čase). Možnost využití krajského hot-spot systému.
* Federované služby autentizace a autorizace (včetně aktivního zapojení do národních 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 zálohování a obnovy dat - SW i HW.
* 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).
* Systémy typu PAM (priviledge access management) a jump-serverů.
* Systémy pro řízení a dohled nad koncovými stanicemi a telefony.

**Nezpůsobilé výdaje**: Vypracování postupů, standardů a politik pro ochranu a řešení bezpečnosti uživatelů, zařízení, infrastruktury a služeb organizace; řádně nezdůvodněné pořízení NetFlow collectoru (k dispozici jako sdílená služba v TCK – FTAS).

**Software**

Cílem projektových aktivit je nákup popř. vývoj a implementace softwarových řešení, které navazují na sdílené služby pro PO provozované krajským úřadem popř. dalšími organizacemi kraje.

**Způsobilé výdaje**:

* Úpravy SW vybavení nutné pro integraci s identity managementem (IDM),
* SW řešení navazující na systém sdílené služby elektronické řídící kontroly (EŘK - Croseus) – úpravy a výměny interních IS (např. ERP/účetnictví),
* SW řešení navazující na systém sdílené služby Facility Management (EMA+),
* SW řešení navazující na systém centrálního nákupu (EZAK),
* SW řešení navazující na systém sdílené služby HelpDesku (ALVAO HelpDesk),
* SW řešení navazující na systém sdílené služby Portálu PO (evidence smluv, kalendář, atd),
* Řešení SW podpory a vybavení pro elektronické podepisování (v souladu s nařízením eIDAS),
* Licence serverového OS,
* Klientské přístupové licence,
* Serverové licence databázových systémů,
* Serverové licence systémů elektronické pošty,
* Náklady na migraci stávajících systémů a dat do sdílených služeb popř. integrace vůči nim.

**Nezpůsobilé výdaje**: podpora a maintenance SW, pronájem SW (SA), cloudové licence, řádně nezdůvodněné pořízení licencí SW provozovaných jako sdílených služeb na KrÚ.

**Virtualizace**

Cílem jsou projekty zaměřené na podporu serverové i klientské virtualizace a technik virtualizace úložišť.

***S ohledem na sdílenou službu hostingu virtuálních serverů musí být součástí žádosti o serverovou virtualizaci zdůvodnění nemožnosti využití hostingu serverů v TCK KrÚ.***

**Způsobilé výdaje**: SW licence virtualizace, HW nezbytný pro běh virtualizačních řešení.

**Nezpůsobilé výdaje**: počítačové stanice a terminály, servery nesouvisející s virtualizací, realizace poskytnutí formou služby (VDI as a service) kromě služeb přímo souvisejících s dodávkou a implementací HW a SW.

**Specifické IT/technické vybavení organizace**

V rámci výzvy lze žádat o pořízení vybavení, které nespadá do žádné z výše uvedených oblastí, a to zejména proto, že je velmi specifické pro provoz příspěvkové organizace a jde o jednorázové, nahodilé pořízení takového vybavení. Součástí žádosti musí být řádně popsané a zdůvodněné HW a SW vybavení, včetně zdůvodnění nutnosti jeho pořízení.

* Příklady: plotery, 3D tiskárny, čidla IoT, technologie energetických úspor, specifický výukový SW, projekční technika, technické vybavení pro zajištění přechodu na DVBT2, nástroje pro zavedení řízené a strukturované zdravotní dokumentace, atd.

**Nezpůsobilé výdaje**: podpora a maintenance SW, pronájem SW (SA), cloudové licence, řádně nezdůvodněné pořízení licencí SW provozovaných jako sdílené služby na KrÚ.

1. *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*](http://www.eduroam.cz/_media/cs/cz_roam_policy_v2.0.pdf)

   [↑](#footnote-ref-2)