

Bod standardu	Popis	Způsob ověření po realizaci
Konektivita školy k veřejnému internetu (WAN)		
1.2.1.	Šíře pásma (bandwidth) odpovídající 0,25 Mbps/žák či student nebo 0,5 Mbps/koncové uživatelské zařízení a zároveň taková šířka pásma, která neomezuje provoz zařízení a uživatelů. Šíře pásma se vztahuje na počet žáků/studentů/koncových uživatelských zařízení v budově/areálu, kde se projekt realizuje.	Smlouva s poskytovatelem připojení.
1.2.2.	Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy.	Příjemce ověří nástrojem na webu www.standardkonektivity.cz a doloží export výsledku a zároveň Smlouva s poskytovatelem připojení.
1.2.3.	Zajištění monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu koncovému zařízení v minimální délce 3 měsíců.	Příjemce doloží nastavení logování požadovaných záznamů ze zařízení a zároveň popíše, jaký mechanismus logování používá (jak loguje a jak dlouho ukládá záznamy).
1.2.4.	Síťové zařízení podporující rate limiting, antispoofing, access listy – zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality.	Příjemce slovně popíše potřebné komponenty a licence pro zajištění řádné funkcionality a zároveň doloží datasheet (produktový list) zařízení, ze kterého bude splnění parametru patrné.
1.2.5.	Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků.	Příjemce slovně popíše potřebné komponenty a licence pro zajištění řádné funkcionality a zároveň datasheet (produktový list) zařízení, ze kterého bude splnění parametru patrné.
1.2.6.	Zajištění šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén pro služby školy dostupné online (např. emailové služby, webové servery, studijní a ekonomické agendy atp.).	Příjemce doloží export z online validátorů https://dnssec-analyzer.verisignlabs.com nebo https://www.dnssec.cz/ (v případě české domény).
1.2.7.	Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem;	Příjemce ověří nástrojem na webu www.standardkonektivity.cz8 a doloží export výsledku
1.2.8.	Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici.	Příjemce popíše systém aktualizace koncových počítačových systémů a softwaru. Uvede, zda jsou aktualizace k dispozici. Pokud aktualizace nejsou k dispozici, uvede, kterého softwaru a firmwaru se to týká.
1.2.9.	Poskytovatel konektivity je schopen zajistit kontaktní bod pro komunikaci, trvalý monitoring dostupnosti konektivity, realizovat blokování nežádoucí komunikace zahrnující nebo jinak omezující konektivitu a systémy školy na straně poskytovatele na základě požadavku školy.	Příjemce doloží smlouvu s poskytovatelem konektivity dokládající naplnění parametru
Vnitřní konektivita školy (LAN a WLAN)		
2.2.1.	Systém 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. službám. Využívání jednoho účtu více uživateli není povoleno (využívání tzv. anonymních účtů).	Příjemce popíše, jak je tento parametr naplněn (zejména to, že je dosaženo bezpečného a auditovatelného přístupu k síti, resp. službám, a to, jakým způsobem je ošetřeno zamezení využívání tzv. anonymních účtů)
2.2.2.	Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém.	Příjemce doloží nastavení logování požadovaných záznamů ze zařízení a popíše, jaký mechanismus logování používá (jak loguje a jak dlouho ukládá záznamy) a zároveň příjemce doloží vnitřní předpis (např. směrnici) zajišťující naplnění parametru.
2.2.3.	Systémy zálohování a obnovy dat serverové infrastruktury.	Příjemce popíše, jak je tento parametr naplněn (zejména popíše technologie a procesy pro zálohování a obnovu dat)

2.2.4.	Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů.	Příjemce doloží fakturu nebo čestné prohlášení dodavatele prokazující nákup služby pro antivirovou ochranu počítačových systémů a antispamovou ochranu poštovních serverů příjemce popíše, jak je tento parametr naplněn (zejména popíše, zda je v organizaci nasazena centrální správa antivirového programu, pokud ano, jaká data ukazuje, dále, jak často je antivirová ochrana aktualizována, jaké hrozby byly detekovány, jaká je platnost licence apod.)
2.3.1.	Minimální konektivita koncových uživatelských zařízení 1000 Mbps full duplex.	Příjemce doloží datasheety (produktové listy) prokazující naplnění parametru a zároveň příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru.
2.3.2.	Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení (např. IPS, IDS, Next Generation Firewall aj.), datových úložišť (NAS) 1000 Mbps full duplex.	Příjemce doloží datasheety (produktové listy) prokazující naplnění parametru a zároveň příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru.
2.3.3.	Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3) 12 s neblokující architekturou přepínacího subsystému (wire speed), management, podpora 802.1Q VLAN (možnost tvorby virtuálních sítí – VLAN), základní bezpečnostní prvky proti zneužití přístupu k síti [např. MAC based omezení (port-sec), 802.1X autentizace aj.].	Příjemce doloží datasheety (produktové listy) prokazující naplnění parametru a zároveň příjemce popíše, jak je tento parametr naplněn (zejména technické parametry používaného hardwaru, zejm. zda podporuje všechny požadované funkcionality, jaká je konfigurace jednotlivých síťových prvků, jak jsou síťové prvky v praxi využívány, příp. ukázka konfigurace na vybraném síťovém zařízení)
2.3.4.	Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.).	Příjemce doloží datasheety (produktové listy) prokazující naplnění parametru a zároveň příjemce popíše, jak je tento parametr naplněn (zejména popíše, jakým způsobem je kabeláž strukturována, jaká kategorie strukturované kabeláže byla použita, případně přiloží projekt)
2.3.5.	Páteřní rozvody mezi budovami v areálu, kde probíhá výuka nebo příprava na ni, realizovány prostřednictvím optických vláken nebo metalických kabelů. Vztahuje se na budovu/areál, kde se projekt realizuje.	Příjemce popíše, jak je tento parametr naplněn (zejména popíše, jakým způsobem je kabeláž strukturována, jaká kategorie strukturované kabeláže byla použita, včetně typu optického vlákna/metalického kabelu, případně přiloží projekt)
2.4.1.	Návrh topologie Wi-Fi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů.	Příjemce doloží smlouvy či jinou dokumentaci prokazující naplnění parametru (návrh topologie, projekt, dokumentace o měření apod. od dodavatele).
2.4.2.	Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu.	Příjemce doloží datasheety (produktové listy) prokazující naplnění parametru příjemce popíše, jak je tento parametr naplněn (zejména popíše konfiguraci centrálního managementu Wi-Fi sítě (security profile) a zda jsou aplikovány požadované parametry)
2.4.3.	Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).	Příjemce doloží vnitřní předpis (např. směrnici) zajišťující naplnění parametru příjemce popíše, jak je tento parametr naplněn (zejména počet oddělených sítí pro konkrétní skupiny, jakým způsobem je zajištěno jejich oddělení, zda podporují VLAN, jaká je konfigurace síťových prvků apod.)

2.4.4.	Podpora mechanismu izolace uživatelů.	Příjemce popíše, jak je tento parametr naplněn (zejména popíše postup v případě zjištění incidentu v síti způsobeného konkrétním uživatelem a blokaci daného uživatele, zanesení na black list)
2.4.5.	Podpora standardu IEEE 802.11ac (Wi-Fi 5) a případně novějších (Wi-Fi 6), současná funkce AP v pásmu 2,4 a 5 GHz a novějších protokolů a pásem.	Příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.
2.5.1.	Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele.	Příjemce doloží nastavení logování požadovaných záznamů ze zařízení a popíše, jaký mechanismus logování používá (jak loguje a jak dlouho ukládá záznamy).
2.5.4.	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 spravovanými access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení).	Příjemce doloží smlouvy či jinou dokumentaci prokazující naplnění parametru (projektová dokumentace, konfigurace centrálního managementu).
2.5.5.	Doporučená podpora pro ověřování uživatelů oproti databázi účtů [např. pomocí protokolu IEEE 802.1X vůči centrální evidenci uživatelů (např. LDAP, MS AD) nebo pomocí Captive portalu].	Příjemce popíše, jak je tento parametr naplněn (zejména popíše způsob ověřování uživatelů, jaké protokoly a centrální evidenci uživatelů využívá, jak jsou nastaveny parametry v centrálním managementu Wi-Fi apod)
2.5.6.	Propojení aktivních prvků a důležitých systémů (např. servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku.	Příjemce doloží datasheety (produktový list) prokazující naplnění parametru.
Další doporučené bezpečnostní prvky projektu		
3.1.4.	Systémy pro monitorování funkčnosti síťové a serverové infrastruktury.	Příjemce popíše, jak je tento parametr naplněn (zejména popíše, jaké systémy jsou využívány)
3.1.8.	Podpora vzdáleného přístupu (VPN).	Příjemce popíše, jak je tento parametr naplněn a zároveň příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.