



**Spolufinancováno
Evropskou unií**



**MINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR**

KUPNÍ SMLOUVA

I. SMLUVNÍ STRANY

1. Kupující: Základní škola a Střední škola CoLibri

se sídlem: Sentice č.p. 215, 666 03 Tišnov

IČO: 08839026

osoba zastupující: Ing. Pavel Matějka, PhD, ředitel školy

Tel.: +420 733 532 890

E-mail: pavel.matejka@skolacolibri.cz

bankovní spojení: Fio banka, a.s., číslo účtu: 400004713/2010

a

2. Prodávající: Data Protection Delivery Center, s.r.o.

zapsaný v obchodním rejstříku vedeném Krajským soudem v Brně,
oddíl C, vložka 83488

se sídlem: Rybkova 1016/31, 602 00 Brno

IČO: 03064247, DIČ: CZ03064247

bankovní spojení: Komerční banka, a.s., číslo účtu: 107-7585660267/0100

osoba zastupující: Ing. Petr Klabeneš, jednatel

tel.: +420 513 034 697

e-mail: obchod@dpdc.cz

kontaktní osoba: Libor Krejčí, tel: +420 731 641 731, e-mail: libor.krejci@dpdc.cz

PREAMBULE

Tuto smlouvu uzavírají výše uvedené smluvní strany na základě výsledku výběrového řízení na veřejnou zakázku malého rozsahu (dále jen "veřejná zakázka") na dodávky s názvem „**ICT vybavení ZŠ CoLibri v souladu se Standardem konektivity**“, zadávanou kupujícím jako zadavatelem dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „zákon o zadávání veřejných zakázek“), v němž byla nabídka prodávajícího vybrána jako nejvýhodnější.

II. ZÁKLADNÍ USTANOVENÍ

1. Tato smlouva je uzavřena na základě výběrového řízení dle pravidel veřejné zakázky malého rozsahu a zadávací dokumentace ze dne 26. 5. 2025
2. Tato smlouva je uzavřena dle § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník (dále jen „občanský zákoník“); práva a povinnosti stran touto smlouvou neupravená se řídí příslušnými ustanoveními občanského zákoníku.
3. Smluvní strany prohlašují, že údaje uvedené v čl. I této smlouvy jsou v souladu s právní skutečností v době uzavření smlouvy. Smluvní strany se zavazují, že změny dotčených údajů oznámí bez prodlení písemně druhé smluvní straně. Při změně identifikačních údajů smluvních stran včetně změny účtu není nutné uzavírat ke smlouvě dodatek.
4. Prodávající prohlašuje, že je odborně a technicky způsobilý k zajištění předmětu plnění podle této smlouvy.
5. Tato veřejná zakázka „Standard konektivity nové budovy odborných učeben pro ZŠ CoLibri | Dodávka je realizovaná v rámci projektu “Vybudování pavilonu odborných učeben a zájmového vzdělávání ZŠ CoLibri“, registrační číslo CZ.06.04.01/00/22-112/0001263, který je spolufinancován ze zdrojů EU, z Evropského fondu pro regionální rozvoj a Integrovaného regionálního operačního programu.

III. PŘEDMĚT SMLOUVY

1. Předmětem smlouvy je závazek prodávajícího provést dodávku předmětu plnění včetně dodání zboží do místa plnění, jeho namontování, instalace, uvedení do provozu a provedení případných dalších prací, dodávek a služeb spojených s realizací předmětu plnění, které jsou definovány zpracovanou technickou specifikací + po sestavení / sešroubování v místě dodání, pokud jsou některé výrobky dodávány složené a rozmontované – v jakosti a množství dle této smlouvy tak, aby dodávka splňovala aktuální verzi standardu konektivity škol. (dále také „Zboží“) a převést na kupujícího vlastnické právo ke Zboží a závazek kupujícího Zboží převzít a zaplatit za něj ujednanou cenu. Nedílnou součástí předmětu smlouvy je: rozmístění, montáž a instalace dodaného vybavení v místě plnění, zprovoznění, monitorování funkčnosti síťové a serverové infrastruktury, předvedení funkčnosti a zaškolení obsluhy.
2. Součástí předmětu plnění je rovněž dodání veškerých dokladů vztahujících se k jeho řádnému užívání, jako jsou návody, technické listy pro užívání a údržbu a dále potřebné certifikáty, předávací protokol a dodací list.
3. Zbožím podle odst. 1 tohoto článku smlouvy se rozumí dodávka IT vybavení do školy dle přílohy č. 1 této kupní smlouvy.
4. Prodávající se zavazuje provést dodávku Zboží vlastním jménem a na vlastní odpovědnost.
5. Veškeré pořizované vybavení bude nové a nepoužité.
6. Kupující trvá na materiálech předepsaných soupisem dodávek a určenými standardy.
7. Prodávající je povinen při plnění povinností vyplývajících ze Smlouvy dodržovat požadavky stanovené podmínkami pro poskytnutí dotace z Dotačního programu IROP, číslo výzvy 112 Zlepšení kvality a dostupnosti sociálních a zdravotních služeb, vzdělávací infrastruktury a rozvoj kulturního dědictví naplnění cíle konektivity tak, aby došlo k úspěšné kontrole naplnění a prokázání Standardu konektivity škol v aktuálním znění, dle přílohy č. 5, 6, 7. Prodávající je povinen při plnění povinností vyplývajících ze Smlouvy poskytovat Objednateli dostatečnou součinnost k plnění povinností stanovených pravidly Standardu konektivity škol, po dobu udržitelnosti projektu tedy 5 let.
8. Prodávající se zavazuje spolupracovat i s dalšími osobami, které určí kupující, tak aby byla zajištěna funkčnost celého díla.

IV. KUPNÍ CENA

1. Cena za provedení celkového předmětu plnění specifikovaného v příloze č. 1 této smlouvy je sjednána jako nejvýše přípustná a činí:
Celkem bez DPH.....1.578.972,00 Kč
 DPH (21 %) 331.584,12 Kč
 Celkem vč. DPH..... 1.910.556,12 Kč
2. Celková cena obsahuje veškeré oprávněné náklady a zisk prodávajícího nezbytné ke včasné a kompletní realizaci předmětu plnění včetně všech souvisejících vedlejších nákladů (tj. náklady na dodání zboží do místa plnění, jeho seřízení, uvedení do provozu + náklady na sestavení / sešroubování v místě dodání, pokud jsou některé výrobky dodávány složené a rozmontované a jakékoliv další náklady spojené s realizací předmětu plnění, které jsou definovány zpracovanou specifikací předmětu plnění). Cena také obsahuje likvidaci obalů a odpadů, nákladů na provedení nezbytných revizí a dodání všech nezbytných dokumentů, práce techniků a dopravného.
3. Smluvní strany v souladu s požadavkem zákona o zadávání veřejných zakázek neumožní změnu smlouvy, která by znamenala podstatnou změnu práv a povinností vyplývajících ze smlouvy. Změny závazku ze smlouvy se řídí pravidly v § 222 zákona o zadávání veřejných zakázek.
4. Je-li prodávající plátcem DPH, odpovídá za to, že sazba daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy; v případě, že dojde ke změně zákonné sazby DPH, bude prodávající ke kupní ceně bez DPH povinen účtovat DPH v platné výši. Smluvní strany se dohodly, že v případě změny kupní ceny v důsledku změny sazby DPH není nutno ke smlouvě uzavírat dodatek.

V. MÍSTO A DOBA PLNĚNÍ

1. Prodávající je povinen odevzdat Zboží v místě plnění, kterým je: obec Předklášteří, parcelní číslo 66/11, 66/10, 312, 63/1, okres Brno-venkov, katastrální území Předklášteří, kraj Jihomoravský.
2. Prodávající se zavazuje odevzdat kupujícímu Zboží dle Harmonogramu, Příloha č.4 takto:
 - Termín dodání dodávky vč. montáže a zprovoznění a zaškolení: **do 5. 9. 2025. (limitní termín)**
 - **Zkušební provoz od 18. 08. 2025 do 30. 09. 2025**

- objednání učiní kupující po ukončení schvalovacího procesu u těch částí Zboží, u kterých je schválení potřebné, viz čl. VI. bod. 2 této Smlouvy. U částí Zboží, které nepodléhá schvalovacímu procesu, proběhne objednání po podpisu Smlouvy bez zbytečného odkladu. Součástí objednávky bude termín dodání, který bude v souladu s tímto článkem Smlouvy, předloženým a od kupujícího schváleným harmonogramem prací, viz příloha č. 4. a potvrzením objednávky vyjadřuje Prodávající s termínem souhlas.

VI. POVINNOSTI PRODÁVAJÍCÍHO A KUPUJÍCÍHO

1. Prodávající dodá technickou dokumentaci k dodanému zboží. Za správnost technické dokumentace a soulad jím dodávaných konstrukcí a výrobků vč. montáže s platnými právními předpisy a požadovanými technickými, kvalitativními vlastnostmi nese prodávající plnou odpovědnost.
2. Prodávající je povinen před dodáním zboží předložit kupujícímu k odsouhlasení seznam výrobků a jejich typové označení. Teprve na základě písemného souhlasu kupujícího a odeslání objednávky od kupujícího dodavateli je možné zahájit dodávku, montáž a instalaci výrobků dle technické specifikace požadované kupujícím.
3. Prodávající kupujícímu odevzdá Zboží, jakož i doklady potřebné k převzetí a užívání Zboží, předávací protokol a dodací list.
4. Dodavatel je povinen odstranit vady do 5 pracovních dnů od jejich nahlášení, ledaže se smluvní strany dohodnou jinak.“
5. Kupující není povinen dodávku Zboží převzít před provedením zkoušek, jimiž bude prokázána řádná funkčnost dodaného Zboží (nebo předvedením Zboží, kterým bude prokázána řádná funkčnost dodaného Zboží).
6. Prodávající je povinen při provádění montáže a seřízení Zboží v místě plnění udržovat čistotu a pořádek. Prodávající odstraní na vlastní náklady odpady, které jsou výsledkem jeho činnosti.
7. Prodávající uvede po ukončení dodávky Zboží všechny plochy dotčené jeho činností do původního stavu. Prodávající je povinen vyklidit místo plnění nejpozději s předáním a převzetím Zboží. Nevyklizení místa plnění se bude považovat za vadu Zboží a kupující není povinen jej převzít.
8. Prodávající je povinen dbát při poskytování plnění dle této smlouvy na ochranu životního prostředí. Dodávané zboží musí splňovat požadavky na bezpečný výrobek ve smyslu zákona č. 102/2001 Sb., o obecné bezpečnosti výrobků a o změně některých zákonů (zákon o obecné bezpečnosti výrobků), ve znění pozdějších předpisů, platné technické, bezpečnostní, zdravotní, hygienické a jiné předpisy, včetně předpisů týkajících se ochrany životního prostředí, vztahujících se na výrobek a jeho výrobu.
9. Kupující je povinen zaplatit kupní cenu podle článku II. této smlouvy a převzít dodávku Zboží podle této kupní smlouvy.
10. Kupující není povinen převzít dodávku Zboží, pokud prodávající neprokáže, že její technické parametry odpovídají hodnotám požadovaným ve specifikaci předmětu plnění a zajištění standardu konektivity škol dle přílohy č. 5, 6, 7,
11. Kupující se zavazuje poskytnout prodávajícímu místo plnění tak, aby prodávající na něm mohl provést instalaci Zboží a jeho seřízení v souladu s podmínkami smlouvy.
12. Prodávající se zavazuje provádět činnosti uvedené v této smlouvě tak, aby nenarušoval chod školy a provoz budovy.
13. Prodávající se zavazuje k tomu, že ke dni podpisu této smlouvy má uzavřenou pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou prodávajícím třetí osobě, a to ve výši **min. 2 mil. Kč**. Tato pojistná smlouva musí být platná po celou dobu trvání této smlouvy i po dobu záruční lhůty. V případě zániku této pojistné smlouvy je prodávající povinen neprodleně o této skutečnosti informovat kupujícího a uzavřít novou pojistnou smlouvu ve stejném rozsahu. Pojistná smlouva bude předložena kupujícímu k nahlédnutí ke dni podpisu této smlouvy, případně pokud kupující stanovil jinou dodatečnou lhůtu, nejpozději však k datu zahájení plnění. **Nepředložení dokladů o pojištění kupujícímu, je považováno za porušení smlouvy, které opravňuje kupujícího k odstoupení od této smlouvy.**
14. Prodávající je povinen zajišťovat plnění podle čl. III odst. 1 této smlouvy. Pokud předmět plnění nezajišťuje prodávající sám, je to povinen zajistit výhradně prostřednictvím poddodavatelů, které uvedl ve své nabídce v rámci veřejné zakázky. V případě, že prodávající v souladu se zadávací dokumentací dané veřejné zakázky prokázal splnění části kvalifikace prostřednictvím poddodavatele, musí tento poddodavatel i tomu odpovídající část plnění poskytovat. Prodávající je oprávněn změnit poddodavatele, pomocí kterého prokázal splnění části kvalifikace, jen za závažných důvodů a s předchozím písemným souhlasem kupujícího, přičemž nový poddodavatel musí disponovat minimálně stejnou kvalifikací, kterou původní poddodavatel prokázal za prodávajícího; kupující nesmí souhlas se změnou poddodavatele bez objektivních důvodů odmítnout, pokud mu budou příslušné dokumenty předloženy.

VII. PŘEVOD VLASTNICKÉHO PRÁVA A NEBEZPEČÍ ŠKODY NA ZBOŽÍ

1. Kupující nabývá vlastnické právo ke zboží dnem jeho převzetí od prodávajícího v místě plnění; v témže okamžiku přechází na kupujícího nebezpečí škody na zboží.

VIII. PŘEDÁNÍ A PŘEVZETÍ ZBOŽÍ

1. Zboží se považuje za odevzdané kupujícímu jeho převzetím kupujícím v místě plnění dle čl. V této smlouvy. Je-li součástí závazku prodávajícího montáž/instalace zboží nebo seznámení s obsluhou zboží, považuje se zboží za odevzdané až po jejich provedení a převzetí zboží kupujícím dle předchozí věty.
2. Kupující při převzetí zboží provede kontrolu:
 - a) dodaného druhu a množství zboží,
 - b) zjevných jakostních vlastností zboží,
 - c) zda nedošlo k poškození zboží při přepravě,
 - d) dokladů dodaných se zbožím.
 - e) Splnění standardu konektivity
3. V případě zjištění zjevných vad zboží může kupující odmítnout jeho převzetí, což řádně i s důvody potvrdí na dodacím listu.
4. O předání a převzetí zboží prodávající vyhotoví dodací list, který za kupujícího podepíše k tomu pověřený zástupce. Prodávající je povinen na dodacím listu uvést typ zboží, počet kusů, sériové číslo zboží (pokud existuje) včetně zobrazení v podobě čárového kódu a datum předání. Dodací list bude dále obsahovat jméno a podpis prodávající osoby za prodávajícího a jméno a podpis přejímající osoby za kupujícího. Dodací list bude označen číslem této smlouvy, uvedeným kupujícím v jejím záhlaví. Prodávající odpovídá za to, že informace uvedené v dodacím listu odpovídají skutečnosti. Nebude-li dodací list obsahovat údaje uvedené v tomto odstavci, je kupující oprávněn převzetí zboží odmítnout, a to až do předání dodacího listu s výše uvedenými údaji.

IX. PLATEBNÍ PODMÍNKY

1. Kupující nebude poskytovat zálohy. Cena dodávky Zboží bude uhrazena až po dodání zboží do místa plnění, jeho seřízení, uvedení do provozu + po sestavení / sešroubování v místě dodání, pokud jsou některé výrobky dodávány složené a rozmontované a po odstranění všech případných vad a nedodělků na základě sepsaného předávacího protokolu. O předání a převzetí provedené dodávky Zboží sepiší strany předávací protokol.
2. Splatnost daňového dokladu (faktury) je **30 kalendářních dnů** od prokazatelného doručení kupujícímu. Faktura se považuje za uhrazenou okamžikem odepsání fakturované částky z účtu kupujícího. Daňový doklad musí obsahovat všechny povinné náležitosti definované zejména v § 28 odst. 2 zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění a zákona č. 563/1991 Sb., o účetnictví, v platném znění.
3. Kupující může vrátit daňový doklad v případě, kdy daňový doklad vykazuje formální nedostatky nebo nevzniklo právo na vystavení takového daňového dokladu na příslušnou částku. V případě, že daňový doklad (faktura) nebude mít odpovídající náležitosti, je kupující oprávněn zaslat ho ve lhůtě splatnosti zpět prodávajícímu k doplnění či úpravě, aniž se tak dostane do prodlení se splatností, lhůta splatnosti počíná běžet znovu od opětovného prokazatelného doručení náležitě doplněného či opraveného dokladu. Prodávající bere na vědomí, že kupující má v úmyslu spolufinancovat plnění, jež je předmětem této smlouvy, z prostředků Evropské unie a státního rozpočtu prostřednictvím Ministerstva pro místní rozvoj ČR v rámci programu „Integrovaný regionální operační program“ tzn. že na daňových dokladech musí být mimo jiné uvedena tato informace, že se jedná o projekt spolufinancovaný z prostředků Evropské unie a státního rozpočtu prostřednictvím Ministerstva pro místní rozvoj ČR v rámci programu „Integrovaný regionální operační program“ spolu s registračním číslem projektu: CZ.06.04.01/00/22-112/0001263.
4. Smluvní strany se dále dohodly, že v případě, že se prodávající stane ve smyslu ust. § 106a zákona o dani z přidané hodnoty nespolehlivým plátcem daně a po dobu, kdy za něj ve smyslu uvedeného zákonného ustanovení bude považován (tedy až do doby, kdy bude rozhodnuto, že není nespolehlivým plátcem daně), bude kupující oprávněn hradit účtované části ceny předmětu plnění co do částky, odpovídající dani z přidané hodnoty, přímo na účet správce daně. Poukázáním příslušné částky na účet správce daně se v dané části bude považovat účtovaná částka za uhrazenou.
5. Nebude-li faktura obsahovat některou povinnou nebo dohodnutou náležitost nebo bude chybně vyúčtována cena nebo DPH, je kupující oprávněn fakturu před uplynutím lhůty splatnosti vrátit druhé smluvní straně k provedení opravy s vyznačením důvodu vrácení. Prodávající provede neprodleně opravu vystavením nové faktury. Vrácením vadné faktury prodávajícímu přestává běžet původní lhůta splatnosti. Nová lhůta splatnosti běží ode dne doručení nové faktury kupujícímu.

X. ZÁRUKA ZA JAKOST A PRÁVA Z VADNÉHO PLNĚNÍ

1. Záruční doba na dodávku a montáž Zboží činí 24 měsíců, pokud není specifikováno jinak v příloze č. 1 a začíná běžet dnem předání Zboží uvedeným v předávacím protokolu. Po dobu záruky odpovídá dodavatel za to, že předané vybavení, které je součástí předmětu smlouvy bude prosté jakýchkoli vad a bude mít vlastnosti sjednané touto smlouvou. Po dobu záruky zajistí dodavatel technickou podporu (servis v době záruky, poradenství, nastavení systému, podpora v případě závady apod.) v rozsahu podrobně specifikovaném u jednotlivých položek cenového a technického formuláře.
2. Záruka za jakost představuje závazek, že dodané Zboží bude po dobu trvání záruční doby způsobilé pro použití k obvyklému účelu. Záruka za jakost se nevztahuje na vady způsobené kupujícím v důsledku porušení ustanovení této smlouvy, instrukcí obsažených v dokumentaci dodávané se Zbožím nebo jeho částí či jiných doporučení prodávajícího.
3. Smluvní strany se dohodly, že v případě vad, které se vyskytnou v záruční době, má kupující právo požadovat a prodávající povinnost odstranit vady zdarma. Náklady na odstranění vad ve sporných případech nese prodávající až do rozhodnutí soudu.
4. Vadou se rozumí odchylky v kvalitě, množství a parametrech stanovených zadávacími podmínkami, touto smlouvou a obecně závaznými technickými normami a předpisy.
5. Proávající se zavazuje neprodleně zahájit odstraňování oznámených vad a vady odstranit v nejkratší technicky možné době; vady znemožňující užívání dodaného Zboží se prodávající zavazuje odstranit nejpozději do 48 hodin od oznámení vady, pokud se obě smluvní strany nedohodnou jinak.
6. Veškeré náklady spojené s odstraněním záručních vad nese prodávající. Jestliže prodávající neodstraní vady v termínech dle odst. 5, je kupující oprávněn, kromě uplatnění smluvní pokuty, podle vlastního uvážení tyto práce provést sám, pověřit jejich provedením třetí osobu, nebo jejím prostřednictvím zakoupit, vyměnit vadnou či neúplně funkční část dodávky Zboží. Takto vzniklé náklady je prodávající povinen zaplatit kupujícímu do 14 dnů od doručení faktury. Takto odstraněné vady budou považovány za odstraněné prodávajícím a prodávající ponese dál záruku za celé dílo v plném rozsahu dle této smlouvy, včetně vad odstraněných třetí osobou.
7. V případě nesplnění povinnosti podle odstavce 5 tohoto článku nese prodávající odpovědnost za škodu, která tím kupujícímu vznikne nebo kterou budou na kupující v této souvislosti uplatňovat třetí osoby. Veškeré takto vzniklé náklady uhradí kupujícímu prodávající.
8. Kupující má právo na odstranění vady dodáním nové věci nebo opravou; je-li vadné plnění podstatným porušením smlouvy, také právo od smlouvy odstoupit. Právo volby plnění má kupující.

XI. SANKCE

1. Neodevzdá-li prodávající kupujícímu zboží ve lhůtě uvedené v čl. V odst. 2 této smlouvy, je povinen zaplatit kupujícímu smluvní pokutu ve výši **0,1 %** z kupní ceny bez DPH uvedené v čl. IV odst. 1 této smlouvy, a to za každý započatý den prodlení.
2. Pokud prodávající neodstraní vadu zboží ve lhůtě uvedené v čl. X odst. 5 této smlouvy, je povinen zaplatit kupujícímu smluvní pokutu ve výši **0,1 %** z kupní ceny bez DPH podle čl. IV odst. 1 této smlouvy, a to za každý započatý den prodlení až do odstranění vady.
3. Pro případ prodlení se zaplacením kupní ceny sjednávají smluvní strany úrok z prodlení ve výši stanovené občanskoprávními předpisy.
4. Smluvní pokuty se nezapočítávají na náhradu případně vzniklé škody, kterou lze vymáhat samostatně vedle smluvní pokuty, a to v plné výši.

XII. ZVLÁŠTNÍ USTANOVENÍ

1. Proávající je povinen uchovávat veškeré doklady, které souvisí s realizací projektu a jeho financováním (dle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů), nejméně po dobu 10 let od finančního ukončení projektu, nejméně však do 31. 12. 2035. Pokud je v českých právních předpisech stanovena lhůta delší než v evropských předpisech, musí být použita pro úschovu delší lhůta.
2. Tato povinnost se vztahuje i na veškeré poddodavatele, které prodávající využije při plnění této smlouvy. Proávající odpovídá za to, že tuto povinnost smluvně přenese na všechny své poddodavatele, a to nejpozději při zahájení jejich plnění.

3. Finančním ukončením projektu se rozumí den, ke kterému je uskutečněna poslední platba spojená s realizací projektu ze strany řídicího orgánu a veškeré finanční prostředky/dotace jsou proplaceny na účet příjemce (tj. kupujícího). Kupující je povinen o této skutečnosti informovat prodávajícího do 10 pracovních dní.
4. Dodavatel se zavazuje, že při plnění této smlouvy bude plně respektovat pravidla ochrany osobních údajů dle GDPR a zabezpečení ICT v souladu s platnou legislativou.
5. Kupující prohlašuje, že uznává e-mailovou komunikaci na mail info@skolacolibri.cz za vhodnou a dostačující pro efektivní řešení záležitostí týkající se plnění této Kupní smlouvy.

XIII. ZÁNÍK SMLOUVY

1. Tato smlouva zaniká:
 - a) písemnou dohodou smluvních stran,
 - b) jednostranným odstoupením od smlouvy pro její podstatné porušení druhou smluvní stranou, s tím, že podstatným porušením smlouvy se rozumí zejména:
 - neodevzdání zboží kupujícímu ve stanovené době plnění,
 - pokud má zboží vady, které je činí neupotřebitelným nebo nemá vlastnosti, které si kupující vymínil nebo o kterých ho prodávající ujistil,
 - nedodržení smluvních ujednání o záruce za jakost nebo o právech z vadného plnění.
2. Kupující je dále oprávněn od této smlouvy odstoupit v těchto případech:
 - a) bylo-li příslušným soudem rozhodnuto o tom, že prodávající je v úpadku ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů (a to bez ohledu na právní moc tohoto rozhodnutí);
 - b) podá-li prodávající sám na sebe insolvenční návrh.
3. Odstoupením od smlouvy není dotčeno právo oprávněné smluvní strany na zaplacení smluvní pokuty ani na náhradu škody vzniklé porušením smlouvy.
4. Pro účely této smlouvy se pod pojmem „bez zbytečného odkladu“ dle § 2002 občanského zákoníku rozumí „nejpozději do 14 dnů“.

XIV. ZÁVĚREČNÁ USTANOVENÍ

1. Tato smlouva a práva a povinnosti smluvních stran v této smlouvě výslovně neupravené se řídí právními předpisy České republiky, zejména zákonem č. 89/2012 Sb., občanským zákoníkem.
2. Pokud některé ustanovení této smlouvy (zcela nebo zčásti) je nebo se stane nezákonné, neplatné nebo nevymahatelné, zůstávají ostatní ustanovení v plném rozsahu platné a účinné.
3. Smluvní strany si ujednávají, že v případě řešení sporných věcí budou přednostně hledat vzájemnou dohodu. Teprve pokud se nedohodnou, obrátí se na příslušný soud.
4. Smluvní strany výslovně vylučují použití jakýchkoliv obchodních zvyklostí ve svém právním styku v souvislosti s touto smlouvou.
5. Prodávající bere na vědomí, že kupující je povinným subjektem dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění. Prodávající souhlasí s tím, že kupující může poskytovat informace týkající se poskytování plnění dle této smlouvy ve smyslu výše uvedeného zákona č. 106/1999 Sb.
6. Prodávající bere na vědomí, že si kupující, jakožto zadavatel, vyhrazuje právo uveřejnit podle § 219 zákona č. 134/2016 Sb. na svém profilu tuto smlouvu včetně jejích změn a dodatků, výši skutečně uhrazené ceny za plnění veřejné zakázky, jež je předmětem této smlouvy, a případně seznam poddodavatelů prodávajícího.
7. Doplňování nebo změnu této smlouvy lze provádět jen se souhlasem obou smluvních stran, a to pouze formou písemných, postupně číslovaných a takto označených dodatků.
8. Smluvní strany prohlašují, že osoby podepisující tuto smlouvu jsou k tomuto úkonu oprávněny.
9. Prodávající nemůže bez souhlasu kupujícího postoupit svá práva a povinnosti plynoucí ze smlouvy třetí straně.
10. Smlouva je vyhotovena v jednom elektronickém originálu, pokud nebude stanoveno jinak.
11. Prodávající si je vědom, že je ve smyslu zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, povinen spolupůsobit při výkonu finanční kontroly. Prodávající se ve spolupráci s kupujícím zavazuje poskytnout kontrolním orgánům jakékoliv dokumenty vztahující se k realizaci projektu, podat informace a umožnit vstup do svého sídla a

jakýchkoliv dalších prostor a na pozemky související s projektem nebo jeho realizací. Prodávající se zavazuje poskytnout na výzvu své daňové účetnictví nebo daňovou evidenci k nahlédnutí v rozsahu, který souvisí s projektem. Prodávající se dále zavazuje provést v požadovaném termínu, rozsahu a kvalitě opatření k odstranění kontrolních zjištění a informovat o nich příslušný kontrolní orgán, kupujícího a poskytovatele dotace.

12. Prodávající bere na vědomí, že poskytovatel dotace je oprávněn provést u projektu nezávislý vnější audit. Prodávající je povinen při výkonu auditu spolupůsobit. Povinnost poskytnout informace a dokumentaci vztahující se k projektu se vztahuje na zaměstnance nebo zmocněnce pověřených orgánů (tj. CRR, Ministerstva pro místní rozvoj ČR, Ministerstva financí ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, Auditního orgánu, Platebního a certifikačního orgánu finanční správy a dalších oprávněných orgánů státní správy) minimálně do roku 20235.
13. Prodávající se dále zavazuje písemně poskytnout na žádost kupujícího jakékoliv doplňující informace související s realizací projektu, a to ve lhůtě stanovené kupujícím. Prodávající poskytne součinnost pro zpracování monitorovacích ukazatelů pro poskytovatele dotace.
14. Účastníci prohlašují, že tato smlouva byla sepsána podle jejich pravé a svobodné vůle, nikoli v tísní nebo za jinak jednostranně nevýhodných podmínek. Smlouvu si přečetli, souhlasí bez výhrad s jejím obsahem a na důkaz toho připojují své podpisy.
15. Tato smlouva nabývá platnosti a účinnosti dnem jejího podpisu smluvními stranami.
16. Nedílnou součástí této smlouvy jsou přílohy:
 - Příloha č. 1: Položkový rozpočet s technickou specifikací
 - Příloha č. 2: Seznam a specifikace poddodavatelů
 - Příloha č. 3: Doklad prokazující pojištění odpovědnosti prodávajícího
 - Příloha č. 4: Harmonogram prací
 - Příloha č. 5: 220725 Standard konektivity škol final
 - Příloha č. 6: Průvodce ke Standardu konektivity škol
 - Příloha č. 7: Prokázání a kontrola naplnění Standardu konektivity škol

V Předklášteří dne dle el. podpisu

V Brně dne dle el. podpisu

za kupujícího
Ing. Pavel Matějka PhD.

za prodávajícího
Ing. Petr Klabeneš, jednatel

Uchazeč:					VÝROBEK SPLŇUJÍCÍ KRITÉRIA
Parametr	Specifikace	ks	jed. cena bez DPH	celkem	označení
Notebook 15,6"					
Provedení:	Provedení NTB 15.6"	9	11 217 Kč	100 953,00 Kč	Lenovo V15 G4 15.6"FH/i5-13420H/16 G/512/W11 Pro
Baterie:	min. 35Wh				
Paměť:	min. 16 GB DDR 4				
Pevný disk:	min. 512 GB SSD M2 NVME				
CPU:	CPU i5/AMD CPU Passmark min. 17 000				
Konektivita:	Porty min. 4 x HDMI				
Porty	3 x USB 3, 1 x HDMI, 1 x Ethernet port, 1 x Sluchátka, Wífi + BT				
Operační systém:	Win 11				
Klávesnice:	Ano				
Záruka a servis	24 měsíců				
Myš:	Ano				
Tablet/PC 16"					
Provedení:	Tablet/PC 15,6"-16" Dotykový	1	26 086 Kč	26 086,00 Kč	YOGA 7 16"T WQXGA/i7-1360P/16G /1T/INT/W11 Pro
Paměť:	min. 16 GB DDR 4				
Pevný disk:	min. 1 TB SSD M2 NVME				
CPU:	CPI i7/AMD CPU Passmark min 18000				
Konektivita:	Porty min. 4 x HDMI				
Display	min. 2560x1600				
Operační systém:	Win 11				
Ostatní požadavky	HDMI, podpora USB 3.x, bluetooth, Thunderbolt 3, čtečka karet, čtečka otisku prstů, výstup na sluchátka, vstup pro mikrofon, podsvícená klávesnice				
Záruka a servis	36 měsíců				
Notebook 16"					
Provedení:	NTB 16"	2	27 242 Kč	54 484,00 Kč	Lenovo TP E16 G2 16"FH/Ultra7-155H/32 G/1T/W11P
Paměť:	min. 32GB DDR 4				
Pevný disk:	min. 1 TB SSD M2 NVME				
CPU:	CPI i7/AMD CPU Passmark min 24937				
Konektivita:	Porty min. 4 x HDMI				
Display	min. 2560x1600				

Operační systém:	Win 11 Pro				
Ostatní požadavky	HDMI, podpora USB 3.x, bluetooth, čtečka otisku prstů, výstup na sluchátka, vstup pro mikrofon, WIFI, BT,				
Záruka a servis	36 měsíců				
Notebook s MacOS 14,2"					
Provedení:	NTB 14,2" Full HD, IPS				
GPU	Integrovaná GPU grafika, rozlišení display 3024 x 1964				
Paměť:	24 GBDDR4				
Pevný disk:	1 TB				
CPU:	10 Core, min 3,9 Ghz, CPU Passmark min. 24000	1	60 859 Kč	60 859,00 Kč	MacBook Pro 14" M4 10xCPU/10xGPU/24G/1T/CZ/SLV
Konektivita:	Wifi 802.11a/b/g/n/ac/, BT 5.3				
Porty:	2 x USB 4 / Thunderbolt				
Operační systém:	MAC OS				
Záruka a servis	24 měsíců				
Stolní PC					
Provedení:	Tower				
GPU	Integrovaná GPU grafika, Grafika 10 GPU				
Paměť:	32 GBDDR4				
Pevný disk:	1 TB SSD				
CPU:	AMD/ Intel, Core 8, min 3,4 Ghz, CPU Passmark min. 26000	1	29 500 Kč	29 500,00 Kč	Stolní PC X-DIABLO Gamer AM4, Ryzen 7 5700X, 2 x 16GB, 1000TB SSD, GIGABYTE RTX™ 4060 Ti, W11 PRO
Grafická karta	16 GB Cache, 2 x HDMI, 1 x DP				
Konektivita:	Wifi 802.11a/b/g/n/ac/, BT 5.3				
Porty:	2 x USB 4 , 1x RJ 45,				
Operační systém:	Windows 11 Pro				
Záruka a servis	24 měsíců				

Tablet 10"					
Provedení:	Tablet min 10,9", Wifi, Dotykový	8	8 990 Kč	71 920,00 Kč	iPad 10,9" Wi-Fi 64GB Silver
Grafika	QHD 2360 × 1640				
Paměť:	4 GB				
Pevný disk:	64 GB				
Konektivita:	Wifi, BT, USB -C				
Operační systém:	iPAD os				
Záruka a servis	24 měsíců				
Projektor do Sálu					
Minimální parametry:	Laserové projekční řešení (20 000 hodin),Technologie 3LCD, RGB se závěrkou s kapalnými krystaly,Jas 5 200 lumenů Ostrý obraz a jasné barvy i v plně osvětlených místnostech,Rozlišení WUXGA Ostrý obraz s rozlišením Full HD zaručuje vynikající čistotu,16:10; kontrast 2 500 000 :1;korekce Manuální vertikální: ± 30 °, Manuální horizontální ± 30 °;shift Manuální - Vertikální ± 50 %, horizontální ± 20 %; Možnosti připojení připravené na budoucí nároky Podpora vstupu 4K, HDMI, HDBaseT, vestavěné rozhraní Wi-Fi a funkce screen mirroring;Rozhraní USB 2.0-A, USB 2.0, RS-232C, Ethernetové rozhraní (100 Base-TX / 10 Base-T), bezdrátová síť LAN IEEE 802.11a/b/g/n/ac (WiFi 5), bezdrátová síť LAN b/g/n (2,4 GHz), bezdrátová síť LAN a/n (5 GHz), VGA vstup (2x), VGA výstup, HDMI výstup, HDBaseT, Miracast, audiovýstup, stereofonní konektor mini-jack, audiovstup (2x), HDMI (HDCP 2.3) (2x), Přehrávání USB 2 typu A	1	59 827 Kč	59 827,00 Kč	EPSON EB-L530U
Požadované příslušenství:	držák na strop délky do 15cm				
Instalace	kompletní instalace včetně příslušenství, potřebné kabeláže, instalace a konfigurace software, oživení a zaškolení obsluhy				
Ozvučení Sálu - zesilovač					

Minimální parametry:	výstupní výkon 2× 600 W / 20 – 20 000 Hz, THD 0.03 %, 8 Ω, režim Stereo, nebo Parallel výstupní výkon 1× 1700 W / 20 – 20 000 Hz, THD 0.03 %, 8 Ω, režim Bridge dva monofonní kanály s displejem, robustní provedení, třída zesilovače H (= AB + řízení napájecího napětí) frekvenční rozsah 20 – 20 000 Hz / ± 0,5 dB, poloviční výkon vstupní citlivost ±0,707 V odstup S/N > 100 dB / A, plný výkon zkreslení THD+N < 0,03 %, plný výkon zkreslení IMD < 0,04 % / 60 Hz, 7 kHz tlumení > 400 / 8 Ω, 100 Hz rychlost přeběhu 40 V / us vstupní impedance 10 kΩ vstupní konektory symetrické XLR výstupní konektory (odbočky vstupů) symetrické XLR pro napojení dalšího zesilovače výstupní konektory Speakon – 4 pin a šroubovací elektronické ochrany proti přetížení, zkratu, stejnosměrnému napětí na výstupu, přehřátí jistič napájení, popř. pojistka soft start – pomalý náběh napájecího napětí zpožděné připnutí reprosoustav řízené chlazení ventilátorem, předozadní vestavěný limiter a filtr velmi nízkých a velmi vysokých frekvencí přepínač režimu zesilovače Stereo / Parallel / Bridge vestavěná subwooferová výhybka s nastavením dělicí frekvence a možností vypnutí indikace zapnutí, signálu, limitace a aktivity ochrany pro každý kanál podsvětlený LCD displej se zobrazením nastavené hlasitosti a teploty chladiče pro každý kanál otvory pro instalaci do 19" rozvaděče (racku) max.rozměry 482 × 89 (2U) x 445 mm max.zastavěná hloubka 407 mm	1	14 640 Kč	14 640,00 Kč	DEXON DAH 1700
Instalace	kompletní instalace včetně příslušenství				

Ozvučení Sálu - reprosoustavy					
Minimální parametry:	dvoupásmová reprosoustava se širokým vyzařováním basový reproduktor 10" s grafitovanou membránou 2 středovýškové 4" reproduktory výkon 150 W rms / 300 W max. impedance 8 Ω frekvenční rozsah 40 – 20 000 Hz / –10 dB citlivost 90 dB / 1W, 1m max. hladina akustického tlaku SPL 112 dB / 1 m široké vyzařovací úhly 120° vertikálně x 120° horizontálně bassreflexová ozvučnice ozvučnice z odolného plastu – polypropylenu dělicí frekvence výhybky 1,2 kHz strmost výhybky 12 dB / oct. elektronická ochrana reproduktorů 3 otvory se závitem M8 pro instalaci držáku pérková připojovací svorkovnice s paralelním odbočením na druhou reprosoustavu pracovní teplota –25 – +60 °C stupeň krytí IP 44 max.rozměry 550 × 336 × 316 mm max.hmotnost 9 kg / ks	4	8 153 Kč	32 612,00 Kč	DEXON SP 1032
Požadované příslušenství:	držák na stěnu				
Instalace	kompletní instalace včetně příslušenství a potřebné kabeláže				
Ozvučení Sálu - mixažní pult					

Minimální parametry:	Mixážní pult se 2 mono a 2 stereo vstupy. Mono vstupy nesymetrické i symetrické přes konektory Jack 6,3 a XLR. Technická data vstupy mono / stereo: 2 / 2; efektová cesta (Jack 6,3): mono Send / stereo Return; Cd/Tape vstup: 2× Cinch; zařazení Cd/Tape vstupu: odposlech / hlavní; výst. na odposlech: Jack 6,3; výstup hlavní: Jack 6,3; výstup na nahrávání: 2× Cinch; výstup na sluchátka: Jack 6,3; potenciometry výstupů: 1 + 1; indikace výstup. signálu: led bargraf; fadery: odolné ALPS; frekvenční rozsah: 10 – 60 kHz / ± 3 dB; zkreslení: THD+N < 0,01 % / A; odstup S/N: 112 dB; napájení: adaptérem; výbava mono vstupů: sym. / nesym. přes XLR nebo Jack 6,3 + 3 pásmový frekvenční korektor + nastavení vst. citlivosti + nastavení panoramy + nastavení úrovně do efektové cesty + sepnutelné fantomové napájení; citlivost mono vstupu – 40 dBu - +10 dBu; výbava stereo vstupů: nesym. přes Jack s nastavením hlasitosti a vyvážení + 3 pásmový frekvenční korek-tor + nastavení úrovně do efektové cesty; nastavení frekvenčního korektoru: 80 Hz; 2,5 kHz; 2 kHz / ± 15 dB; max. výstupní úroveň master: + 22 dBu	1	4 021 Kč	4 021,00 Kč	DEXON DMC 2220
Instalace	kompletní instalace včetně příslušenství a potřebné kabeláže				

Ozvučení Sálu - modul internetového rádia a streamování v LAN, WiFi a Bluetooth					
Minimální parametry:	streamování internetových rádií, podcastů a hudby z internetových úložišť streamování hudebního obsahu z místní sítě LAN pomocí DLNA, AirPlay streamování lokální hudby ze smartphone nebo tabletu, kde se nachází streamovací aplikace streamování hudby s připojené flash paměti na slot USB-A, verze USB 2.0, max. kapacita 4 GB streamování prostřednictvím Bluetooth 5.0 konektivity poslech linkového vstupu Aux s konektorem Jack 3,5 stereo systémově nezávislé streamování. Nezáleží na systému (iOS, Android, Blackberry, Windows...), nad kterým běží streamovací aplikace, protože se využívá univerzálních protokolů komunikace otevřený systém, audio je možné přehrávat pomocí různých aplikací, např. 4Stream, Múzo Player, Air Wire, All Connect a dalších, nebo rovnou prostřednictvím aplikací internetových služeb jako jsou např. Spotify nebo TuneIn. Streamovat je možné obvykle i přímo z „továrních“ přehrávačů smartphonů a tabletů. Všeobecnou podmínkou je, aby aplikace měly možnost vybírat UPnP zařízení v síti a streamovat přes DLNA nebo AirPlay. podpora streamovacích protokolů AirPlay, DLNA, Qplay, Spotify Connect podpora síťových protokolů TCP/IP, UDP podpora hudebních formátů Mp3, WMA, WAV, ALAC, AAC, AAC+, FLAC, APE ethernet připojení do LAN přes konektor RJ 45, max. přen. rychlost 10 / 100 Mb/s WiFi konektivita 802.11 b/g/n, pásmo 2,4 GHz, max. přen. rychlost 150 Mb/s modul může fungovat jako WiFi zařízení typu AP (Access point = vytváří svou WiFi), STA (modul přihlášen do jiné WiFi), AP Client (modul vytváří svou WiFi a současně je přihlášen do jiné WiFi) audio výstup Line Out konektorem Jack 3,5 stereo audio vstup Aux In konektorem Jack 3,5 stereo, vstupní citlivost 1 V rms (-3,8 dBu) vícebarevná LED indikace zvoleného způsobu streamování: USB / Bluetooth / Net / Aux In dosah Bluetooth přijímače 15 m dekódování ze vzorkování až 24 b / 192 kHz frekvenční rozsah 20 – 20 000 Hz / – 0,5 dB odstup S/N > 91 dB slot mikroUSB-B pro napájení DC 5 V, napájecí adaptér AC 230 V / DC 5 V / 1 A je součástí balení max .rozměry 117 × 23 × 65 mm	1	6 300 Kč	6 300,00 Kč	DEXON JWS 11
	Instalace	kompletní instalace včetně příslušenství a potřebné kabeláže			
Ozvučení Sálu - bezdrátový mikrofon diverzitní ruční + náhlavní / klopový, 2kanálový do racku					

Minimální parametry:	obsahuje přijímač, 1 ruční mikrofon, 1 vysílač za opasek, 1 náhlavní mikrofon, 1 klopový mikrofon, v jednom okamžiku lze provozovat 2 mikrofony diverzitní UHF tunery, 2 kanály, PLL zpětný IR přenos pro snadné automatické nalazení a spárování pomocí funkce SYNC funkce proskenování celého pásma SCAN indikace 2x nalazení na nosnou, 2x audio vybuzení, 2x číslo kanálu, 2x naladěné frekvence, 2x tuneru diverzitního modu, uzamčení podsvětlený LCD displej regulace úrovně hlasitosti každého kanálu kompresor, expander, 2 šumové brány separátní sym. výstupy konektory XLR a celkový nesym. výstup konektorem Jack 6,3 výstupní úroveň 300 mV ef. / nesym, ±150 mV ef. / sym. 10 kΩ možnost nastavení SQUELCH příjmových podmínek pro každý kanál zvlášť funkce uzamčení nastavení využívá frekvenční pásmo 640 – 660 MHz, pro nalazení je k dispozici až 100 frekv. kanálů. Tím odpadají problémy s naladováním dokupovaných vysílačů a se sestavováním složitějších kombinací pohromadě. Taktéž na vysílačích (ručních mikrofonech nebo vysílačích za opasek) se nastavuje 1 ze 100 možných frekvencí. Toto nastavení lze provést manuálně nebo automaticky pomocí funkce SYNC, kdy přijímač zpětně, pomocí IR přenosu, „sdělí“ vysílači, kde se má naladit. Přímou v souladu s všeobecným oprávněním VO-R/10/07.2021–8 ČTÚ šířka pásma < 200 kHz frekvenční rozsah audio 35 – 16 000 Hz frekvenční stabilita ± 0,005% FM (F3E) modulace zkreslení THD < 0,5 % dynamika > 100 dB odstup S/N > 90 dB IR čidlo pro párování a automatické nastavení podle přijímače odnímatelné antény na konektorech BNC (bajonet) držáky pro instalaci přijímače do 19" racku napájení adaptérem (je součástí) DC 13 – 18 V / 0,5 A včetně transportního kovového kufru max.rozměry 420 × 41 (1U) x 205 mm	1	13 860 Kč	13 860,00 Kč	DEXON MBD 732
Instalace	kompletní instalace včetně příslušenství a potřebné kabeláže				

INTERAKTIVNÍ PANEL 75" včetně příslušenství					
Úhlopříčka:	min.190 cm(75")				
Rozlišení:	min.4K UHD(3840x2160 pixelů při 60Hz)				
Dotyková technologie:	technologie InGlass IR, antireflexní + oleofobní + antimikrobiální temperované sklo,min. tvrdost 7H (tužka), min.20 souvislých dotykových bodů pro Android a 40 pro Windows,podpora multitouch, ovládání dotykem ruky i stylusem, přesnost dotyku do 1,2 mm, doba odezvy do 8 ms, nástroje pro psaní - pero, prst, dlaň, součástí min.2 ks bezbateriových per.				
Ostatní parametry:	minimální : 1 slot pro integrovatelný (OPS) počítač, kontrast (dynamický) 5000:1, obnovovací frekvence 60 Hz, pozorovací úhel 178°, jas 400 cd/m2, snímač okolního světla,vnitřní operační paměť 8GB, uložení 128GB, verze Android 13.0, osmijádrový procesor				
Vstupy:	min.vstup HDMI 2.0 (4K@60Hz) x2, Display port 1.2 x1; USB-A 3.0 (Android)x1, USB-A 3.0 x2,USB-B 3.0 (Touch)x2, LAN in (RJ45, 10/100/1000 Mb/s)x1 ,LAN out (RJ45, 10/100/1000 Mb/s)x1 , RJ-232 (Serial) x1, USB-C 3.0 x1, modul Wi-Fi (IEEE 802.11a/b/g/n/ac 2x2), bluetooth 5.0, výstup HDMI 2.0 (4K@60Hz) x1, vstup pro mikrofon (3,5 mm)x1, slot pro kameru				
Ozvučení:	min.2x20W				
Záruka:	v minimální délce 24 měsíců s možností rozšíření v rámci udržitelnosti projektu na 60 měsíců od výrobce				

Interaktivní funkce a software:	Panel automaticky rozpozná stylus (psaní), prst (manipulace s objekty) i dlaň (mazání). A to přímo v prostředí kancelářských aplikací Office 365. Vše zcela přirozeně, jako byste používali pero a papír. 20 souvislých dotykových bodů, gesta a potažení prstem od okraje obrazovky. Součástí jsou základní aplikace pro výuku včetně licence, kompatibilita s operačními systémy, používanými na škole. Aplikace bílá tabule – s celou řadou praktických nástrojů. Bez nutnosti připojovat počítač. Možnost přihlášení pomocí QR kódu a rychlého uložení svých poznámek na Disk Google. Možnost Importu obrázků z webu přímo do tabule, matematické nástroje, lístečky s poznámkami. Možnost použití tabule více žáky současně. Nástroje tabule pro vytváření poznámek lze používat samostatně v rámci výuky, webového prohlížeče nebo jiného obsahu. Sdílení obrazovky - Prezentuje a sdílí bezdrátově obsah přímo z vašeho zařízení. Podporuje všechny běžné notebooky, tablety, telefony a prohlížeče. Umožňuje i obousměrnou komunikaci, při které je možno na panelu nejen prezentovat, ale i přímo od dotykové obrazovky váš počítač bezdrátově ovládat. Nemusí být ani na stejné síti, postačí libovolné připojení k internetu. Vysílání obsahu obrazovky všem posluchačům (Sdílení obsahu vašeho zařízení) jakémukoliv připojenému účastníkovi. (až 200 posluchačů). Možnost se k vysílanému obsahu připojit se svým zařízením z jedné místnosti, učebny, posluchárny nebo z jakéhokoli jiného místa, kde je přístup k internetu. Správa všech panelů z jednoho místa - Jednoduché ovládání všech panelů na dálku. Možnost nastavovat funkce obrazovky, instalovat aplikace, používat funkci „Digital Signage“ (vzdálené plánování a ovládání obsahu) a odesílat zprávy na jednotlivé obrazovky nebo jejich skupiny. Interaktivní výukový nástroj, pomocí něhož lze nativně importovat své stávající výukové materiály včetně souborů IWB, SMART Notebook a flipchartů Promethean. Importovat lze jakýkoli obsah, obrázky, video, PDF, PowerPoint, text, tvary a mnoho dalšího. Aplikace Nástroje - výběr nejpoužívanějších nástrojů ze strany učitelů, jako je časovač, opona, bodový reflektor, kostka a semafor. Tento widget funguje po otevření jako překryvný prvek. Lze jej minimalizovat, přepínat mezi libovolnými obrazovkami a otevřít nabídku nástrojů, kdykoli je třeba.	1	87 879 Kč	87 879,00 Kč	NEWLINE LYRA PRO75" + BalanceBox 400
Požadované příslušenství:	Manuální posuvný systém pro interaktivní panel. Instalace (zavěšení) pouze na čelní stěnu bez kontaktu s podlahou. Min. zdvih 40cm,				
Instalace	kompletní instalace včetně příslušenství, potřebné kabeláže do 15m, instalace a konfigurace software, oživení a zaškolení obsluhy				
Ostatní Příslušenství					
Dokovací stanice	USB-C Dokovací stanice, 135W, USB porty, 3x USB 3.1, 2x USB 2.0, 1x USB -C, Audio porty, Kombinovaný audio jack, Ethernet Gigabit Ethernet	6	4 658 Kč	27 948 Kč	ThinkPad USB-C Dock 135W
Monitor - 27" USB-C	min. 27", poměr 16:9, Rozlišení: min 2560x1440, 1000:1, Soundbar, USB HUB (USB 3.2 Typ B / DisplayPort, HDMI), obnovovací frekvenci min. 60Hz, odezva max. 4ms / 36 měsíců	4	8 040 Kč	32 160 Kč	Lenovo P27q-30 27"IPS/16:9/2560x1440/1000:1/350 + Sounbar

Monitor - 27" 4K	min. 27" IPS/16:9/3840:2160, 1300:1, Rozhraní USB, USB-C / DisplayPort, HDMI, USB-C, frekvenci min. 60Hz, odezva max. 4ms./ 36 měsíců	2	9 820 Kč	19 640 Kč	Lenovo T27p-30 27" IPS/16:9/3840:2160/1300:1/4ms
Monitor - 34" UltraWide - Prohnutý	min. 34", 3440 x 1440 WQHD, min 175 Hz při 0,1ms, formát 21:9, min 1000 cd/m2,min. 10 bit barevná hloubka , Porty: 2x HDMI, 1x DisplayPort, 1x USB-C, VESA /36 měsíců	1	18 593 Kč	18 593 Kč	34" LED Philips 34M2C8600 - QD-OLED,USB-C,ambiglow
Tiskárna	A3 velká kancelářská síťová barevná Laser Multifunkce (tisk, kopy, scan, posílání na email, uložit na USB). Podavač na mnohostránkové oboustranné skenování a tisk. Připojení min.: LAN, Wifi, USB, Rozlišení barevného tisku: 1800 x 600, 1200 x 1200, rozlišení při kopírování a skenování 600 x 600, rychlost skenování min 100str/min, zásobník min 1000str., gramáž papíru i 300g/m2, Interní paměť: min 2GB,Disk: min256 GB, Barevný model: CMYK, min 17 tisíc stran na ČB toner a min 11 tisíc stran při barevném tisku obě při 5% pokrytí, AirPrint (iOS), možnost uživatelských schránek s heslem, šifrování dat uživatelů, podpora IEEE 802.1x.Dodání s plnými originálními tonery.	1	70 272 Kč	70 272 Kč	Develop Ineo+ 251i
Klávesnice:	Klávesnice drátová: - Klávesnice odolná proti polití - 3zónová klávesnice v kompaktním provedení - Klávesy ostrovního stylu pro lepší přesnost a pohodlí - Optická myš s rozlišením 1200 dpi - Bezdrátové připojení 2,4 GHz přes nano USB přijímač	6	700 Kč	4 200 Kč	
PC myš	Myš bezdrátová, 1200DPI, 3 tlačítka, symetrická, optická	6	300 Kč	1 800 Kč	
Sluchátka	Frekvenční rozsah: 30-16.000 Hz;Sluchátka s elektretovým mikrofonom s funkcí umlčení šumu pro volnou komunikaci před osobním počítačem;Ideální pro telefonování, hlasem ovládané programy a počítačové hry u zvukových karet s vestavěným napájením;Technologie umlčující šum "Clear Voice TechnologyTM" zajišťuje čistou komunikaci v rušném prostředí;Molitanové náušníky pro otevřený, vzdušný zvuk;Nastavitelný hlavový most pro maximální pohodlí;Impedance mikrofону 2,2 ohmy;citlovost min.91 dB;Délka přívodního kabelu je 2,5 m	1	737 Kč	737 Kč	Koss CS100
Celkem				175 350 Kč	

Virtualizační server					
Provedení serveru:	Rack server s možností konverze do 19"racku, max. 2U nedělené chassis 16 x 2,5"	1	212 760 Kč	212 760 Kč	PowerEdge R550 Se
Počet procesorových patič na server:	Min. osazen 1x procesor poslední dostupné generace				
Počet jader na fyzický procesor:	min. 16 core,				
Požadovaný minimální výkon procesoru:	Min. 29200 dle PassMark CPU Benchmark (single CPU)dle https://www.cpubenchmark.net, Perfomance Test V10				
Operační paměť (osazení) na server:	Min. 16 paměťových slotů - pozic - pro RAM ,Osazení min. 4x 64GB DDR4 2666MHz				
Disková kapacita:	Hot plug disky,Osazeno min. 5 x 1,92 TB SSD SATA Read Intensive 6Gbps				
RAIDový řadič:	HW RAID řadič , Raid 0, 1, 10, 5 s podporou Hot Spare + Cache				
Ethernet konektivita na server:	Minimálně 2 x 1Gb port onboard nebo na přídatvné PCIe kartě				
Ventilátory:	Redundantní hotswapové ventilátory				
Napájení a spotřeba:	Redundantní hot-plug napájecí zdroje, každý s maximálním výkonem 600W a účinností alespoň 94% - Platinum, ke každému zdroji napájecí šňůra.				
Porty:	1 Gb Dedicated Management Network Port, USB 3.0 x1, USB 2.0 x1 3 x PCIe Gen 3 slots x16				
	Součástí licence pro virtualizaci až na 4 VM;Součástí liece Windows server Standard 2025;Součástí 120 Uživatelských licencí				
Záruka a SW licence:	Na 60 měsíců, s Odezvou následující pracovní den				
UPS					
Provedení UPS:	tower s umístěním do rack	1	25 933 Kč	25 933,00 Kč	Eaton 9SX 1000i Rack2U
LCD panel:	Informační LCD Panel na přední straně				
Výkon:	1000 VA				
Typ UPS:	Online/ Dvojitá koverze				
Ostatní:	Kompatibilní s dodávaným serverem a SW;Management karta pro připojení do LAN				
Záruka a servis	36 měsíců				
Zálohovací uložště včetně SW					
Procesor:	Min. 4 Core, min. 2,2 GHz	1	76 088 Kč	76 088,00 Kč	Synology RS822RP+ Rack Station - 4x 4T, Nakivo
Paměť:	Min. 8 GB RAM				
Pevné disky:	Min. 4 x 4 TB SATA HDD				
Ethernet:	Min. 4 x 1 gbit/s				
Porty:	2 x USB 3.2 Gen 1.;1 x Gen3 x8 slot (x8 link)				
Příslušenství:	Lyžiny do RACK				
Sw:	Součástí SW pro zálohování všech dat z VM na 5 let				
Záruka a servis	Na 36 měsíců				

Monitoring Sítového provozu				
Provedení:	Ucelený škálovatelný NetFlow/IPFIX monitorovací systém, schopný monitorovat síťový provoz jak na fyzické síťové infrastruktuře, tak i v rámci instalovaného virtuálního prostředí. Získané statistiky o provozu datové sítě musí umožnit sledovat a vyhodnocovat objemy a strukturu provozu, analyzovat příčiny provozních nebo výkonnostních problémů a odhalovat bezpečnostní hrozby. Je nezbytné, aby monitorovací systém byl zcela nezávislý na použité síťové infrastruktuře a svou funkcí monitorovanou síť neovlivňoval Kompletní instalace ve virtuálním prostředí s možností v případě potřeby rozšířit o hardwarové sondy (tj. podpora decentralizovaného monitoringu)			
Datové toky:	Bezeztrátová kontrola každého jednotlivého paketu, podpora NetFlow v5, NetFlow v9 – RFC3954, IPFIX, jFlow, cflowd, NetStream, IPv4, IPv6, VLAN, NAT, MPLS, MAC			
Viditelnost:	Ze strany sledované sítě nesmí být monitorovací systém detekovatelný			
Management:	Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS, uživatelsky přívětivé GUI.			
Reporting a alertování:	E-mailové notifikace, SNMP trapy, Agregace událostí. Nástroj pro generování a zaslání uživatelsky definovaných grafických reportů			
Uložný prostor:	Možnost uložit minimálně 500 GB zachycených dat s možností navýšení rozšířením licence			
Ukládání dat:	Kontinuální ukládání dat bez jakékoliv ztrátové agregace (bez ohledu na požadovanou dobu ukládání)			
Nastavení času:	Časová synchronizace zařízení proti centrálnímu zdroji času na síti	1	125 000 Kč	125 000 Kč
Konektivita:	min. 2x 1Gbs dedikovaná konektivita do síťové infrastruktury			
Externí datové zdroje:	Provázání monitorovaných dat s Active Directory			
Možnosti rozšíření:	Modulární řešení umožňující doplnění o další funkcionality (detekce DoS, plný záchyt síťového provozu, bezpečnostní analýza chování v síti, monitoring výkonu aplikací, monitoring síťové infrastruktury, atd.).			
API:	Otevřené rozhraní a dokumentované API s možností integrace nástrojů i třetích stran			
Uživatelé:	Správa uživatelů a přístupových práv			
Zákaznická podpora:	Plná zákaznická podpora v českém jazyce			
Další požadavky:	Jsou požadovány software aktualizace (nové verze programového vybavení) v minimální délce 5 let. - Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.			
Min. požadované konfigurační práce:	Instalace do virtuálního prostředí a jeho odpovídající nastavení			
	Konfigurace páteřního přepínače pro sběr monitorovaných dat a integrace s firewall			
	Základní konfigurace systému (IP adresa, uživatelské účty, snmp, smtp, ntp, syslog, kvóty, profily)			
	Provázání monitorovaných dat s Active Directory, tj. spárování IP adresy se jménem autentizovaného uživatele			
Provozní monitoring				
Monitorování prostředí	Síťové zařízení: Monitorování routerů, switchů a dalších síťových komponentů. Servery: Podpora pro monitorování fyzických a virtuálních serverů.			

	Aplikace a služby: Monitorování různých aplikací a služeb (např. webové servery, databázové servery). Cloudové služby: Podpora pro monitorování cloudových prostředí a služeb (např. AWS, Azure). Agenti: Použití agentů pro shromažďování a odesílání metrik z monitorovaných systémů. Bezagentní monitoring: Shromažďování dat pomocí SNMP, IPMI, a dalších protokolů bez potřeby instalace agenta. Skriptování: Možnost spouštění vlastních skriptů pro shromažďování a monitorování dat. Pravidla upozornění: Možnost definovat pravidla pro generování upozornění na základě prahových hodnot a událostí. Kanály upozornění: Podpora pro e-maily, SMS, webhooks, a integrace s nástroji jako Slack nebo PagerDuty. Eskalace upozornění: Možnost konfigurace eskalačních plánů a postupného upozorňování. Uchovávání dat: Uchovávání historických dat a metrik pro analýzu a reportování. Vyhledávání a filtrace: Možnost vyhledávání a filtrování historických událostí a metrik. Grafy a diagramy: Zobrazení historických dat a trendů pomocí grafů, diagramů a tabulek. Trendy a analýzy: Analýza trendů a výkonu na základě historických dat. Šifrování: Podpora šifrování komunikace mezi agenty, servery a uživatelskými rozhraními. Autentizace a autorizace: Možnost použití různých metod autentizace a správy uživatelských přístupů. Zálohování a obnova: Možnost zálohování konfigurace a dat, obnova po havárii. Mapy: Vizualizace topologie sítě a fyzického umístění zařízení. Šablony: Použití a přizpůsobení šablon pro standardizaci monitorování. Včetně implementace provozního monitoringu Automatizace: Automatické přidávání a konfigurace nových zařízení pomocí šablon.	1	15 000 Kč	15 000 Kč	Monitoring ZABBIX
--	---	---	-----------	-----------	-------------------

Software:					
Antivirus:	SW licence pro antivirovou ochranu počítačů požadujeme: - centrální správa produktu jak onprem, tak cloud nevázané na licenci - Podpora operačních systémů MS: Windows 8.1, Windows 10, Windows Server 2012, Windows Server 2012R2, Windows Server 2016. ▪ Antivirový klient také pro ochranu systémů: Linux, macOS, Android. ▪ Real-Time ochrana před všemi druhy malwaru: Viry, červy, trojskými koňmi (backdoor, adware, spyware, rootkit, bootkit, ransomware...). ▪ Napojení na centrální správu: Kompletně v češtině, Možnost dovoufaktorového ověření do konzole – Možnost expirace hesla u uživatelů konzole – Vzdálená instalace z centrální konzole, několika způsoby: Instalace z konzole, Instalace balíčku přes GPO – Možnost spustit Network discovery z kteréhokoli již instalovaného klienta – uživatelů, nebo skupin (např. administrátorů) v AD. ▪ Možnost blokáce/whitelistace přístupu na definované weby, nebo skupiny webů dle kategorií s možností whitelistování na uživatele nebo skupiny v AD. ▪ Antivirus a Antispyware pro aktivní ochranu před všemi typy hrozeb. ▪ Ochrana proti podvodným a phishingovým webovým stránkám ▪ Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID ▪ Anti-Phishing blokující webové stránky s podvodnými formuláři pro vylákání citlivých údajů a stránky obsahující škodlivý kód. ▪ HIPS pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost zařízení. ▪ Jsou požadovány software aktualizace (nové verze programového vybavení) v minimální délce 5 let	40	2 500 Kč	100 000,00 Kč	ESET 5y
Instalační a konfigurační práce					
	Konfigurace Firewall FG90 v souladu se standardem konektivity škol (je již vlastněn školou)	1	45 000 Kč	45 000 Kč	
	Nasazení Helpdesk	1	15 000 Kč	15 000 Kč	
	Instalace a konfigurace switchů, včetně vytvoření VLANů a napojení na L2/L3 switch v souladu se standardem konektivity škol (je již vlastněn a namontován školou)	1	35 000 Kč	35 000 Kč	
	Nastavení LAN v souladu se standardem konektivity škol	1	29 000 Kč	29 000 Kč	
	Instalace server, nasazení virtualizační platformy	1	35 000 Kč	35 000 Kč	
	Instalace MS AD, File server	1	19 000 Kč	19 000 Kč	
	Nasazení NAS a zálohování	1	18 000 Kč	18 000 Kč	
	Nasazení Síťové sondy v souladu se Standardem konektivity	1	20 900 Kč	20 900 Kč	
	Kompletní dokumentace ke splnění standardů konektivity škol	1	39 000 Kč	39 000 Kč	
	Instalace PC a NTB, implementace OS a zapojení do školní sítě	1	25 000 Kč	25 000 Kč	
	Instalace UPS	1	5 000 Kč	5 000 Kč	
	Celkem	1		285 900 Kč	

Celkem bez DPH				1 578 972,00 Kč
21% DPH				331 584,12 Kč
Celkem včetně DPH				1 910 556,12 Kč

Poznámka k technické specifikaci:	Pokud jsou v technické specifikaci obsaženy požadavky nebo odkazy na jednotlivá obchodní jména, zvláštní označení podniku, zvláštní označení výrobků, výkonů anebo obchodních materiálů, která platí pro určitý podnik nebo organizační jednotku za příznačné, popř. patenty a užitné vzory, jsou uvedeny pouze pro upřesnění a přiblížení technických parametrů a zadavatel umožňuje použití i kvalitativně a technicky obdobného nebo lepšího řešení. Uvedené konkrétní číselné hodnoty u jednotlivých položek jsou stanoveny jako fixní a nabízené zařízení musí tyto parametry splnit. Vyjimkou jsou ty položky kde je uvedeno, že se jedná u minimální hodnotu(min.). Zde může uchazeč nabídnout lepší hodnotu konkrétního parametru. Pro splnění uvedených požadavků již žádné další softwarové licence než ty, které jsou výše specifikovány nejsou požadovány. Záruka na všechny položky je 24 měsíců pokud není u položky jiná specifikace.
Poznámka ke způsobu vyplnění přílohy	Uchazeči povinně vyplní barevně (modře) označené buňky.



Prohlášení – seznam a specifikace poddodavatelů

na akci „ ICT vybavení ZŠ CoLibri v souladu se Standardem konektivity “

- I. * Účastník zadávacího řízení nemá v úmyslu zadat žádnou část veřejné zakázky jednomu či více poddodavatelům v souladu se zadávacími podmínkami.
- II. * ~~Účastník zadávacího řízení má v úmyslu zadat jednu nebo více částí veřejné zakázky jednomu či více poddodavatelům v souladu se zadávacími podmínkami, dle níže uvedené specifikace:~~

podíl v % podíl v Kč

PRÁCE REALIZOVANÉ VLASTNÍMI KAPACITAMI % Kč

PRÁCE REALIZOVANÉ PODDODAVATELI CELKEM % Kč

INFORMACE O JEDNOTLIVÝCH PODDODAVATELÍCH:

Název společnosti, právní forma a přesná adresa:	druh poddodávky:
.....	
IČ:	 % tis. Kč
.....	
Název společnosti, právní forma a přesná adresa:	druh poddodávky:
IČ:	
..... %	tis. Kč
.....	
Název společnosti, právní forma a přesná adresa:	druh poddodávky:
IČ:	 % tis. Kč
.....	

razítko a podpis oprávněného zástupce uchazeče

- Uchazeč vyplní body I. a II. tohoto prohlášení dle skutečnosti.
- V případě většího počtu poddodavatelů předloží účastník zadávacího řízení jejich specifikaci na více stránkách přílohy č. 2.

* *nehodící se škrtněte*

POTVRZENÍ O POJIŠTĚNÍ / CERTIFICATE OF INSURANCE

CHUBB®

Pojistná smlouva č. / Policy no. **CZINTA25142 – 125**

Pojistník / Policyholder	Data Protection Delivery Center, s.r.o.
	IČ / ID no. 03064247
	Rybškova 1016/31
	602 00 Brno – Veveří Česká republika / Czech Republic
Rozsah pojistného krytí / Risk Exposure	Pojištění profesní odpovědnosti v oblasti informačních technologií / Technology Professional Indemnity Insurance
Územní rozsah / Territorial Limits	Celý svět vyjma USA a Kanada / Worldwide excluding USA and Canada
Limit pojistného plnění / Limit of liability	CZK 10.000.000
Pojistná doba / Term of Insurance	01.04.2025 – 31.03.2026

Ostatní podmínky pojištění se řídí ustanoveními pojistné smlouvy, k níž byl tento certifikát vystaven. Tento certifikát v žádném případě nepozměňuje, nerozšiřuje či nenahrazuje pojistnou smlouvu. / The other terms and conditions of the insurance are governed by the terms of the insurance policy, to which this certificate was issued. In no case does this certificate modify, extend or replace the insurance policy.

V Praze/ In Prague, dne / on 27.03.2025

Pojistitel / insurer: Chubb European Group SE, organizační složka



Chubb European Group SE, organizační složka
Pobřežní 620/3, 186 00 Praha 8
IČ 278 93 723

zapsaná do Obchodního rejstříku
vedeném Městským soudem v Praze,
oddíl A, vložka 57233

.....
Jméno / Name: Erik Macalík

Funkce / position: vedoucí odštěpného závodu / head of the branch

Chubb. Insured.SM

Chubb European Group SE, organizační složka, se sídlem Pobřežní 620/3, 186 00 Praha 8, identifikační číslo 278 93 723, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl A, vložka 57233, je odštěpným závodem společnosti Chubb European Group SE, která se řídí ustanoveními francouzského zákona o pojištění, s registračním číslem 450 327 374 RCS Nanterre a sídlem: La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, Francie. Chubb European Group SE má plně splacený základní kapitál ve výši 896,176,662€. Chubb European Group SE je ve Francii oprávněna k podnikání a regulovaná Autorité de contrôle prudentiel et de résolution (ACPR) 4, Place de Budapest, CS 92459, 75436 PARIS CEDEX 09. Orgánem dohledu pro výkon činnosti v České republice je Česká národní banka; tato regulace může být odlišná od práva Francie.

Osobní údaje, které poskytujete nám [případně vašemu pojišťovacímu makléři] pro upisování, správu zásad, správu pohledávek a jiné účely pojištění, jak je dále popsáno v našich Zásadách ochrany osobních údajů, naleznete zde: [https://www2.chubb.com/cz-cz/privacy.aspx]. Můžete nás kdykoli požádat o tištěnou verzi zásad ochrany osobních údajů a to na emailové adrese [mailto: dataprotectionoffice.europe@chubb.com].

[illegible]

STANDARD KONEKTIVITY ŠKOL

Ministerstvo školství, mládeže a tělovýchovy
červenec 2022

Úvod

Tento dokument definuje základní technická kritéria cílového stavu školní síťové infrastruktury a přijatelnosti aktivit projektů naplňující požadavky na školy v 21. století mj. i strategický cíl IROP 4.1 v oblasti zajištění vnitřní konektivity škol a připojení k internetu - rozvoj vnitřní konektivity v prostorách škol a školských zařízení a připojení k internetu¹.

Další podmínky a pravidla výzev IROP jsou uvedeny ve Specifických pravidel výzev IROP.

Níže uvedené parametry konektivity jsou relevantní pro základní školy, střední školy, vyšší odborné školy a konzervatoře, u kterých Integrovaný regionální operační program 2021–2027 stanovuje ve specifickém cíle 4.1. intervenci v oblasti budování vnitřní konektivity škol.

Metodická podpora ke Standardu konektivity škol je k dispozici na <https://edu.cz/digitalizujeme>.

¹ Viz Programový dokument IROP 2021-2027 (<https://irop.mmr.cz/cs/irop-2021-2027/dokumenty>)

1. Konektivita školy k veřejnému internetu (WAN)

1.1. 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 parametry v době ukončení realizace a v průběhu udržitelnosti projektu.

1.2. Povinné parametry projektu:

- 1.2.1. Šíře pásma (bandwidth) odpovídající 0,25 Mbps/žák či student² nebo 0,5 Mbps/koncové uživatelské zařízení³ a zároveň taková šířka pásma, která neomezuje provoz zařízení a uživatelů⁵. Šíře pásma se vztahuje na počet žáků/studentů/koncových uživatelských zařízení v budově/areálu, kde se projekt realizuje.
- 1.2.2. Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy.
- 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.
- 1.2.4. Síťové zařízení podporující rate limiting, antispoofing, access listy - zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality.
- 1.2.5. Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoku.
- 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.).
- 1.2.7. Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem;
- 1.2.8. Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici.
- 1.2.9. Poskytovatel konektivity je schopen zajistit kontaktní bod pro komunikaci, trvalý monitoring dostupnosti konektivity, realizovat blokování nežádoucí komunikace zahlcující nebo jinak omezující konektivitu a systémy školy na straně poskytovatele na základě požadavku školy.

1.3. Doporučené parametry projektu:

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

- 1.3.1. Symetrické připojení (zajištění konektivity) bez agregace a omezení, doporučujeme postupně směřovat ke kapacitě konektivity 1Gbps.

² Počet žáků/studentů je definovaný celkovým počtem žáků/studentů školy.

³ Koncové uživatelské zařízení je počítačový systém, který je aktivně využíván uživatelem (např. žákem, studentem nebo zaměstnancem školy) ke vzdělávacím či pracovním účelům (typicky počítač, notebook, tablet apod.).

⁴ Metrika vhodná typicky pro školy bez mobilních popř. BYOD zařízení

⁵ Definováno jako saturace šířky pásma připojení k veřejnému internetu, která ani ve špičkách nedosáhne, a to ani krátkodobě 100 %.

- 1.3.2. Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách.
- 1.3.3. Poskytovatel konektivity je schopen zajistit funkci systému incident response, monitoring a aktivní notifikaci anomálií síťového provozu, zamezení podvržení zdrojových IP adres (anti-spoofing), funkci pro blokování nežádoucí komunikace zahlcující nebo jinak omezující konektivitu a systémy školy pro zamezení zahlcení linky (např. RTBH, FlowSpec, služby AntiDDoS řešení), detekci a zamezení amplifikačních útoků, zabezpečení směrování síťového provozu pomocí RPKI a konfigurace odmítnutí nevalidních prefixů.
- 1.3.4. Antivirová kontrola internetového provozu.

2. Vnitřní konektivita školy (LAN a WLAN)

2.1. Obecný popis

Vnitřní síťové prostředí školy pořizované v rámci projektu může být řešeno pevnou sítí, bezdrátovou sítí, nebo kombinací těchto síťových technologií. Připojení je nutné zajistit v prostorách dotčených hlavním projektem, rovněž je možné pokrýt ostatní prostory školy, včetně chodeb, jídelen, internátu a dalších školských zařízení. Potřebnost a účelnost takového pokrytí musí být odůvodněna ve studii proveditelnosti.

2.2. Povinné parametry projektu (bez ohledu typ síťového připojení):

- 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).
- 2.2.2. Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém⁶.
- 2.2.3. Systémy zálohování a obnovy dat serverové infrastruktury.
- 2.2.4. Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů.

2.3. Povinné parametry projektu v oblasti pevné LAN:

- 2.3.1. Minimální konektivita koncových uživatelských zařízení 1000 Mbps full duplex.
- 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.
- 2.3.3. Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3)⁷ s neblokující architekturou přepínacího subsystému (wire speed), management, podpora 802.1Q VLAN (možnost

⁶ Počítačový systém je každý prvek informačních a komunikačních technologií využívající pro svoji činnost jak hardware, tak software. Pro účely standardů jsou rozlišována: 1. koncová uživatelská zařízení (např. osobní počítače, notebooky, tablety, mobily aj.) a 2. servery, síťové prvky, datová úložiště apod.

⁷ 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 architekturu přepínacího subsystému.

tvorby virtuálních sítí - VLAN), základní bezpečnostní prvky proti zneužití přístupu k síti [např. MAC based omezení (port-sec), 802.1X autentizace aj.].

2.3.4. Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.).

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.

2.4. Minimální parametry projektu v případě řešení bezdrátových sítí (WLAN):

2.4.1. Návrh topologie Wi-Fi sítě a analýza pokrytí signálem počítačící s konzistentní Wi-Fi službou v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů.

2.4.2. Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu.

2.4.3. Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).

2.4.4. Podpora mechanismu izolace uživatelů.

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.

2.5. Doporučené parametry projektu (bez ohledu typ sítového připojení):

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

2.5.1. Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele.

2.5.2. Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokace Wi-Fi v určitém čase.

2.5.3. Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací (např. aktivní zapojení do federovaného systému www.eduroam.cz).

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).

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].

2.5.6. Propojení aktivních prvků a důležitých systémů (např. Servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku.

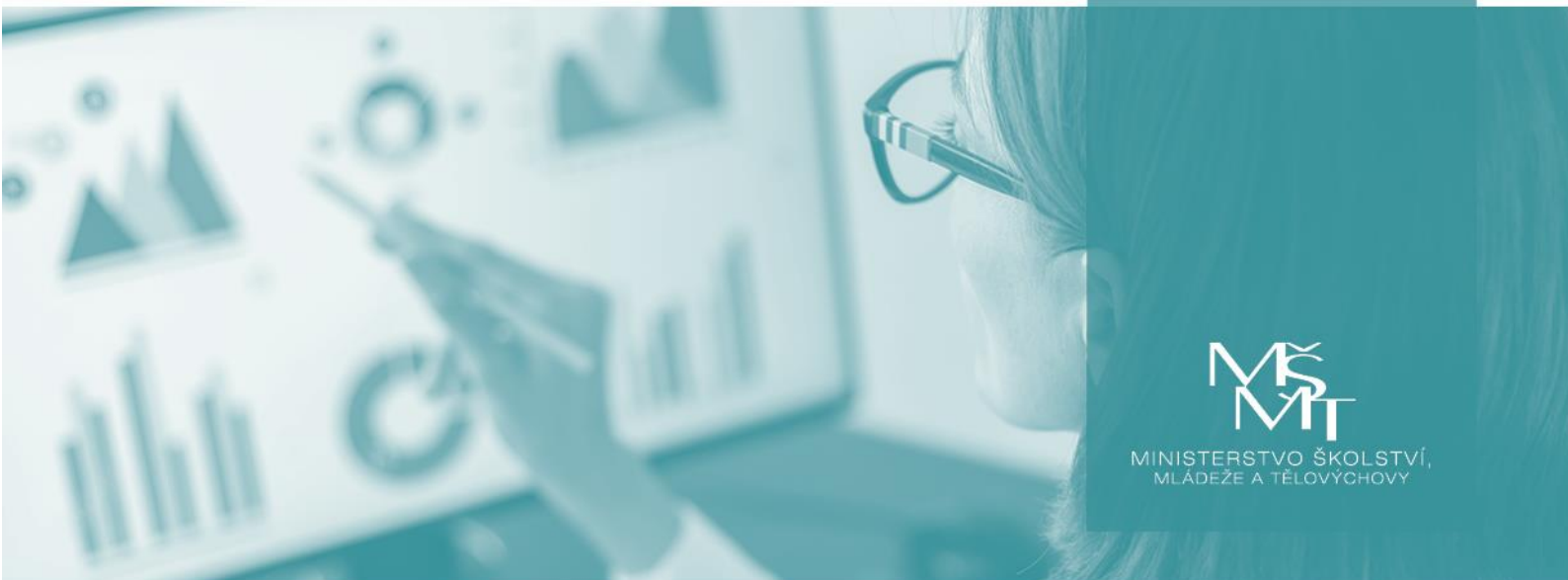
3. Další doporučené bezpečnostní prvky projektu

Nad rámec povinných parametrů uvedených v bodech 1 a 2 je dále doporučeno v projektu realizovat:

3.1.1. Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 - IPFIX nebo ekvivalent).

- 3.1.2. Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie.
- 3.1.3. Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management).
- 3.1.4. Systémy pro monitorování funkčnosti síťové a serverové infrastruktury.
- 3.1.5. Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu.
- 3.1.6. Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk aj.).
- 3.1.7. Nástroje pro centrální správu a audit ICT prostředků.
- 3.1.8. Podpora vzdáleného přístupu (VPN).
- 3.1.9. Zavedení více-faktorové autentizace.

PRŮVODCE KE STANDARDU KONEKTIVITY ŠKOL



MŠMT
MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY

Praha, březen 2024

Č.j. MSMT-27467/2023-1

Obsah

Úvod	3
Konektivita školy k veřejnému internetu (WAN) – vnější konektivita školy	5
Oblast 1: Rychlá a bezpečná přípojka	5
Oblast 2: Firewall	7
Oblast 3: IPv4 adresa	8
Oblast 4: Zabezpečení vnější sítě, šifrování	9
Vnitřní konektivita školy (LAN a WLAN)	11
Oblast 1: Bezpečná správa koncových zařízení	11
Oblast 2: Bezpečné ukládání a správa dat školy	16
Oblast 3: Pevná LAN – připojení koncových zařízení do sítě školy	17
Oblast 4: Řešení bezdrátových sítí (WLAN) – Wi-Fi	19

ÚVOD

Českou společnost, a tedy i vzdělávací systém čekají velké výzvy i příležitosti ve spojitosti s tzv. dvojitou – digitální a zelenou transformací¹. Rychlá digitalizace v posledním desetiletí změnila náš způsob života a pravděpodobně jej bude měnit i nadále. Až 90 % pracovních pozic bude v blízké době vyžadovat alespoň základní digitální dovednosti². V budoucnosti bude čím dál akutnější nedostatek ICT specialistů s pokročilými digitálními dovednostmi, především z oblasti umělé inteligence nebo kyberbezpečnosti.

Cílem vzdělávání je proto v následující dekádě základními a nepostradatelnými kompetencemi vybavený a motivovaný jedinec, který dokáže v co nejvyšší míře využít svůj potenciál v dynamicky se měnícím světě ve prospěch jak svého vlastního rozvoje, tak ve prospěch rozvoje celé společnosti s ohledem na druhé. Poslední roky pro školy představovaly velkou zatěžkávací zkoušku. Pandemie Covid-19 ukázala sílu digitálních technologií, ale i silné či slabé stránky digitalizace. V reakci na globální situaci v pandemii přinesla Evropská komise finanční nástroj, díky kterému v souladu s Národním plánem obnovy Ministerstvo školství, mládeže a tělovýchovy (dále jen „MŠMT“) investuje do digitalizace škol (více viz <https://edu.cz/digitalizujeme>). Počet digitálních zařízení ve školách tak rapidně roste a bude dále růst. Impulzem pro digitalizaci ve vzdělávání je také přechod škol na výuku dle inovovaných školních vzdělávacích programů posilujících informatické myšlení a digitální kompetence.

Ve všech výše popsáných výzvách je nezbytné školy podporovat, a to i ohledně jejich digitální infrastrukturu, která by měla být funkční a bezpečná. Funkčností se v tomto smyslu rozumí především možnost efektivního využívání digitálních technologií ve výuce v souladu s inovovanými školními vzdělávacími programy. Bezpečností se rozumí primárně schopnost čelit hrozbám vnějšího online světa.

MŠMT publikovalo Standard konektivity škol (dále také „Standard“), který je dostupný na webových stránkách <https://edu.cz/digitalizujeme>. Dokument definoval základní technická kritéria cílového stavu školní síťové infrastruktury a přijatelnosti aktivit projektů naplňující požadavky na školy v 21. století, mj. i strategický cíl IROP 4.1 v oblasti zajištění vnitřní konektivity škol a připojení k internetu – rozvoj vnitřní konektivity v prostorách škol a školských zařízení a připojení k internetu.

Cílem Průvodce ke Standardu konektivity škol je blíže školám vysvětlit problematiku digitální infrastruktury školy. Zároveň jim přiblížit důležitost kvality a funkčnosti digitální infrastruktury a pomoci procesu digitalizace vzdělávání. Dokument je určen pro ředitele, ICT koordinátory, správce IT i zřizovatele.

1 https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

2 World Economic Forum. The Future of Jobs. [online]. [cit. 09. 04. 2021]. Dostupné z: http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf

K dispozici jsou i následující metodické materiály:

- **Prokázání a kontrola naplnění Standardu konektivity škol.** Jedná se o dokument pro všechny školy/příjemce, které mají prokázat naplnění parametrů uvedených ve Standardu konektivity škol, dostupný na <https://www.edu.cz/digitalizujeme/standard-konektivity-skol#prokazani>
- **Bezpečná digitální infrastruktura školy.** Dokument, který představuje základní principy, postupy a doporučení v oblasti kybernetické bezpečnosti pro školy. Zároveň je určen IT správcům či administrátorům, dostupný na <https://www.edu.cz/digitalizujeme/bezpecna-skolni-ict-infrastruktura/>
- **Bezpečná školní ICT infrastruktura.** Jedná se o edukační videa, která jsou dostupná na <https://www.edu.cz/digitalizujeme/bezpecna-skolni-ict-infrastruktura/>
- **IT správa.** Příručka ke správě ICT ve škole a příklady dobré praxe (rozhovory i videa), které jsou dostupné na <https://www.edu.cz/digitalizujeme/it-sprava/>.

Nevíte, jak si Vaše škola stojí na poli digitální infrastruktury? Zda je dostatečná, funkční a bezpečná? Obrátte se na specializované IT guru, kteří Vám rádi pomohou a zdarma prověří stav digitální infrastruktury vaší školy. Více informací naleznete na <https://www.edu.cz/digitalizujeme/it-guru/>.

Další informace o metodické podpoře naleznete na <https://www.edu.cz/digitalizujeme/metodicka-podpora/>.

V případě dotazů nás kontaktujte na digitalizujeme@msmt.cz.

Věříme, že Vám tento dokument a další metodická podpora poskytnutá MŠMT a Národním pedagogickým institutem ČR pomůže a bude pro Vás inspirací na cestě digitalizace Vaší školy.

Průvodce dokumentem

Průvodce ke Standardu konektivity škol je rozdělen na dvě části, stejně jako Standard konektivity: vnější konektivita a vnitřní konektivita školy.

Jednotlivé části obsahují oblasti, u kterých je vždy vysvětleno:

Proč? je důležité se jimi zabývat,

-  **Co?** je třeba ze strany školy zajistit
-  **Jak?** návodné otázky, které by měly být položeny.

Technické požadavky, které je třeba pro bezpečnou a funkční digitální infrastrukturu zajistit.

-  **M** minimální úroveň – bez zajištění této úrovně nelze považovat digitální infrastrukturu školy za funkční ani bezpečnou;
-  **S** úroveň Standardu konektivity škol
-  **D** doporučená úroveň a další doporučení

KONEKTIVITA ŠKOLY K VEŘEJNÉMU INTERNETU (WAN) – VNĚJŠÍ KONEKTIVITA ŠKOLY

Proč?

Pro fungování školy v 21. století je nutné zajistit dostatečně kvalitní a bezpečné připojení k internetu. Pandemická situace ukázala vzrůstající nároky na kvalitu nejen vnitřní, ale i vnější rychlosti a kapacity připojení ke světové síti. Toto připojení nesmí zůstat otevřené všemu, je tedy nutné vnitřní svět školy chránit ochrannou zdí, a to tzv. firewalllem, tedy virtuální ochranou mezi sítí internet a vnitřní sítí školy.

Co je třeba zajistit

-  Přístup na internet, který je realizován optickým vláknem, telefonní linkou nebo bezdrátovým spojením (nebo jejich kombinací) v odpovídající rychlosti a kvalitě.
-  Na straně školy je mezi vnitřní a vnější sítí umístěn firewall, který primárně chrání vnitřní síť a zajišťuje bezpečné spojení s „vnějším světem“.
-  Záložní řešení konektivity pro případ, že by došlo k výpadku přístupu k internetu (např. datové simkarty apod.).



OBLAST 1: RYCHLÁ A BEZPEČNÁ PŘÍPOJKA

Proč?

Nároky na připojení v posledních letech nebývale rostou. Jedním z požadavků poslední doby je přenos celé výuky nebo její části do virtuálního prostředí. K zamyšlení proto patří nejen současná rychlost připojení školy, ale také budoucnost rychlosti ve střednědobém horizontu. Jak ale přijít na to, jakou rychlost připojení škola potřebuje nebo bude potřebovat v budoucnu? S touto otázkou vám rádi poradí konzultanti IT guru (<https://www.edu.cz/digitalizujeme/it-guru/>) nebo kolegové z BCO (Broadband Competence Office, <https://www.bconetwork.cz/>).

Návodné otázky:

-  Jakou rychlost přípojky k internetu potřebuji? Bude přípojka stačit i v horizontu 5 let a více s ohledem na plánovaný rozvoj digitální infrastruktury školy?
-  Potřebuji symetrickou přípojku (stejnou rychlost stahování – download a nahrávání dat – upload)?
-  Jaké služby mi poskytovatel konektivity nabízí?

Technické požadavky

Minimální požadavek

- M** Minimální požadavek je stanoven ve Standardu konektivity (parametr 1.2.1).

Standard konektivity škol

- S** Parametr 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.
- S** Parametr 1.2.8 Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici.
- S** Parametr 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.

Doporučení nad rámec Standardu konektivity škol

- D** Směřovat ke kapacitě konektivity školy 1 Gb/s
- D** Symetrická přípojka (stejný download jako upload).
- D** Poskytovatel konektivity je schopen zajistit funkci systému incident response, monitoring a aktivní notifikaci anomálií síťového provozu, zamezení podvržení zdrojových IP adres (anti-spoofing), funkci pro blokování nežádoucí komunikace zahrnující nebo jinak omezující konektivitu a systémy školy pro zamezení zahlcení linky (např. RTBH, FlowSpec, služby AntiDDoS řešení), detekci a zamezení amplifikačních útoků, zabezpečení směrování síťového provozu pomocí RPKI a konfigurace odmítnutí nevalidních prefixů.
- D** Antivirová kontrola internetového provozu.

Další doporučení

- D** Nejlepší možnou variantou je optické připojení, protože poskytuje nejvyšší rychlost připojení.
- D** V případě že není možné optické připojení, doporučujeme snažit se o připojení v co největší možné rychlosti, a to např. bezdrátovou profi technologií, která zajistí kvalitní spojení na co nejbližší bod pátevní sítě internetového poskytovatele. I těmito technologiemi nebývá problém se připojit rychlostmi kolem 100 Mb/s.
- D** V případě škol v lokalitách se sníženou dostupností připojení, je možné využít běžných tarifů od internetových poskytovatelů, využití telefonních linek, které již také dosahují dostatečných kapacit.

- D** Pokud nevíte, jakou rychlost přípojky zvolit, obraťte se na konzultanty IT guru (<https://www.edu.cz/digitalizujeme/it-guru/>).
- D** Pokud si nevíte rady, jaké máte možnosti přípojek ve svém území, spojte se se svým zřizovatelem nebo koordinátorem Broadband Competence Office (BCO, viz <https://bconetwork.cz/>).
- D** Metodické materiály a další informace k vnější konektivitě naleznete na stránkách BCO <https://bconetwork.cz/>.



OBLAST 2: FIREWALL

Proč?

Koncová zařízení a síťové prvky se dostávají do kontaktu s vnější sítí – internetem, a právě odtud hrozí naprostá většina rizik. Firewall je virtuální ochrannou zdí školy před tímto vnějším světem.

Návodné otázky:

- ?** Potřebuji firewall?
- ?** Co vůbec firewall dělá?

Potřebuji firewall?

- I** Ano, firewall je nutný na všech typech škol, které využívají připojení k internetu³.

Firewall – co dělá?

- I** Firewall je prostředníkem mezi vnějším světem a sítí školy.
- I** Správně nastavený firewall neumožní neoprávněný vstup do školní sítě a umožní bezproblémový přístup školní sítě k internetu.
- I** Firewall propustí do vnitřní sítě školy pouze oprávněný provoz a neoprávněné aktivity zastaví.
- I** Firewall na základě pravidel filtruje provoz (přístup) do jednotlivých částí sítě školy.

³ Tato zařízení jsou škálovatelná dle požadavků školy a jsou jednoduchá na pořízení.

Technické požadavky

Minimální požadavek

-  Pořídit a správně nastavit firewall tak, aby nebyl umožněn neoprávněný vstup do školní sítě a zároveň byl zajištěn bezpečný vstup do sítě Internet.
-  Firewall je správně nastaven tak, aby jednotlivé skupiny uživatelů měly přístup do určité části sítě.
-  Firewall je pravidelně/automaticky rekonfigurován na základě zaznamenaných útoků.

Standard konektivity škol

-  Parametr 1.2.5: Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků.



OBLAST 3: IPV ADRESA

Proč?

Veřejná IP adresa školy slouží k jednoznačné identifikaci lokální sítě školy v rámci internetu. V současné době je nejrozšířenější IPv4, z důvodu nedostatku adres je IPv4 postupně nahrazován protokolem IPv6. Veřejná IP adresa je pro školu důležitá z těchto důvodů:

-  Umožňuje IT správci vzdálený monitoring IT infrastruktury, připojení na jednotlivé prvky (routery, servery apod.)
-  Umožňuje zaměstnancům organizace bezpečné připojení do školní sítě zvenku. V případě více budov umožňuje bezpečné propojení a rozšíření vnitřní sítě mezi oddělenými pracovišti.
-  Umožňuje přístup k online systémům školy hostovaných na vlastním hardwaru (např. školský informační systém, stravovací systém apod.)

Návodné otázky

-  Nabízí váš poskytovatel internetu minimálně jednu veřejnou IP adresu v rámci tarifu?

Technické požadavky

Minimální požadavek

-  Minimální požadavek je definován Standardem konektivity škol (parametr 1.2.2).

Standard konektivity škol

- S** Parametr 1.2.2: Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy.

Doporučení nad rámec Standardu konektivity škol

- D** Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách.



OBLAST 4: ZABEZPEČENÍ VNĚJŠÍ SÍTĚ, ŠIFROVÁNÍ

Proč?

Nepřetržitě připojení školy k internetu má za následek její vystavení nehostinnému prostředí a rychle se vyvíjejícím hrozbám. Zaměstnanci a žáci mohou navíc svými činy, ať už úmyslně nebo neúmyslně, interní síť ohrožit, proto je zabezpečení jednou z klíčových činností k ochraně dat organizace. Pro bližší informace k tematice doporučujeme pročíst materiál [Bezpečná digitální infrastruktura školy](#).

Návodné otázky

- ?** Jakým způsobem je síť školy zabezpečena proti vnějším hrozbám a úniku dat?
- ?** Dochází k pravidelnému monitorování síťového provozu a vyhodnocování anomálií?
- ?** Je škola schopna včas identifikovat a zaznamenat kybernetické útoky?

Technické požadavky

Minimální požadavek

- M** Minimální požadavek je definován Standardem konektivity škol (parametry níže).

Standard konektivity škol

- S** Parametr 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.
- S** Parametr 1.2.4 Síťové zařízení podporující rate limiting, antispoofing, access listy – zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality.
- S** Parametr 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.).

-  Parametr 1.2.7 Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem.

Doporučení nad rámec Standardu konektivity škol

-  Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 - IPFIX nebo ekvivalent).
-  Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie.
-  Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management).
-  Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu.

VNITŘNÍ KONEKTIVITA ŠKOLY (LAN A WLAN)

V případě vnitřní konektivity řešíme zabezpečení a kvalitu digitální infrastruktury uvnitř školy, počínaje koncovými zařízeními v majetku školy nebo vlastními zařízeními zaměstnanců a žáků jako jsou počítače, notebooky nebo mobilní telefony, ale i další digitální zařízení jako routery, tiskárny, servery atd. Na těchto zařízeních nakládáme na školách s osobními údaji a dalšími citlivými daty, příkladem jsou matriční záznamy, docházkový a klasifikační systém, účetnictví nebo osobní korespondence. Tyto dokumenty jsou vystaveny nebezpečí i „ze světa“ prostřednictvím internetu, a to i když máme data uložená „pouze“ na vlastním počítači nebo tzv. vnitřní síti. Proto je nutné vnitřní IT provoz chránit a mít ho nastavený tak, aby odolal vnějším i vnitřním hrozbám. Tyto hrozby mohou být automatizované a univerzální nebo cílené a mířit na soukromá a citlivá data vás nebo vašich žáků. Následky mohou být ekonomické až likvidační, zároveň mohou narušovat soukromí zaměstnanců a žáků nebo ohrožovat vývoj a psychiku jedince. Za žádných okolností tedy nelze toto riziko podceňovat.



OBLAST 1: BEZPEČNÁ SPRÁVA KONCOVÝCH ZAŘÍZENÍ

Proč?

Uživatel přistupuje k vnitřní síti nebo internetu pomocí jednotlivých koncových zařízení (notebook, stolní počítač, tablet, mobil apod.). Z vnějšku je tak i se svým zařízením vystaven rizikům. Na druhou stranu, jakmile se připojuje k síťovým zařízením školy, působí tato koncová zařízení jako riziko. V každém případě tedy musí být zabezpečená samotná zařízení. Čím dál větší výzvou je zvládnutí správy s ohledem na vzrůstající počet těchto zařízení a různorodosti hrozeb. Řešením může být tzv. centrální řízení účtů (viz níže).

Zároveň se ve školní síti pohybují různí uživatelé, kteří by měli mít přidělená správná oprávnění. Cílem je zajistit například to, aby žáci nemohli do adresářů učitelů nebo vedení školy a učitel měl přístup do adresářů, které potřebuje k výkonu své práce, nebo aby se nestalo, že se neoprávněná osoba dostane do klasifikačního systému a provede nežádoucí úpravy. Vše musí být správně zabezpečeno a v souladu s GDPR.

Co je potřeba zařídit:

- I** Nastavit systém pro pravidelné aktualizace software koncových zařízení – zejména aktualizace operačního systému zařízení tak, aby byly pravidelně řešeny minimálně kritické opravy operačního systému.
- I** Vhodně zvolený způsob logování (přihlašování do sítě školy) tak, aby se případné incidenty daly zpětně dohledat.
- I** Vhodně zvolený způsob logování (přihlašování do sítě školy) tak, aby se nepovolání uživatelé nedostali do částí sítě, které jim nepřísluší.

-  Účty administrátorů a účty běžných uživatelů jsou odděleny (nelze mít účet, který používá učitel pro svou práci mezi administrátory).
-  Žádný koncový uživatel (žák, pedagog, nepedagog, host) nemá na koncovém zařízení žádná administrátorská oprávnění.
-  Každý uživatel má přidělenou správnou sadu oprávnění.
-  Vhodně zvolená antivirová ochrana zařízení.
-  Bezpečné zapojování mobilních zařízení v majetku školy, které uživatelé používají i mimo školní síť (například zapůjčené zařízení).
-  V případě, že škola zvolila přístup BYOD⁴, je ošetřeno bezpečné zapojení mobilních zařízení do sítě školy.
-  V interní směrnici školy je ošetřeno nakládání s nepoužívanými účty a daty (např. v případě odchodu žáka či zaměstnance), zejména by mělo být specifikováno, po jaké době se účet a data po odchodu mažou/deaktivují.
-  Počet anonymních účtů by měl být minimalizován, příp. eliminován.
-  U všech účtů by mělo být řešeno nastavení: délky, složitosti a intervaly vypršení hesla, neopakovatelnosti hesel při změně a zamykání účtů při neúspěšných pokusech o přihlášení.
-  Přístup do BIOS⁵ je omezen heslem a zavedení operačního systému je umožněno pouze z pevného disku. Disk v notebookech a PC by měl být šifrován.

Návodné otázky

-  Potřebuji centrální řízení účtů? Jsme schopni zajistit aktualizaci, zabezpečení a funkčnost každého koncového zařízení ve škole ručně?
-  Jaký způsob řešení centrálního řízení účtů je pro naši školu vhodnější? Univerzální cloudový balíček pro školství, serverový systém nebo kombinace?
-  Je zajištěn přístup do sítě tak, aby nebylo možno zneužít administrátorský účet?
-  Dostane se každý uživatel v síti jen tam, kam smí?
-  Řešíme účty zaměstnanců/žáků, kteří již ve škole nejsou?

4 Z anglického Bring Your Own Device, tzn. žáci ve výuce pracují s vlastními digitálními zařízeními (např. mobilem, tabletem nebo počítačem).

5 BIOS (z angl. Basic Input/Output Setup) slouží k nastavení/detekci komponent a spolupráce základní desky s operačním systémem. Zdroj: https://it-slovník.cz/pojem/bios/?utm_source=cp&utm_medium=link&utm_campaign=cp



Co je to centrální řízení účtů?



Důvodem pro zavedení centrální správy účtů v organizaci je snaha zvýšit bezpečnost, produktivitu a zároveň snížit náklady a opakující se úkony při správě stejných účtů v rozličných aplikacích napříč organizací. Každému uživateli v síti je umožněno přihlásit se pomocí jeho unikátního přihlašovacího jména a hesla na jakoukoliv jemu povolenou stanici či do aplikace.

Centrální řízení účtů umožňuje:



Jednotnou správu účtů uživatelů a správců s možností nastavení konkrétních oprávnění pro přístup k systémům či jen k datům v rámci sdílených úložišť apod.



Rozdělovat účty do skupin s různými oprávněními přístupu.



Nastavit více-faktorovou autentizaci pro určitou skupinu účtů (doporučeno pro administrátorské účty).



Mít přehled o jednotlivých stanicích.



Server nebo univerzální cloudové balíčky pro školství?



Centrální řízení účtů lze vyřešit dvěma způsoby, které mají své výhody a nevýhody a dají se i vzájemně kombinovat:

a) Univerzální cloudové balíčky pro školství (např. MS Office 365 Education nebo Google Workspace for Education⁶),

- Pro školy jsou zdarma. Je však i tak třeba počítat se správou.
- Škola nemusí mít v budově fyzické servery, o ty se stará poskytovatel služby.
- Data a informace školy mohou být však reálně uložena na serverech, které jsou někdy mimo ČR nebo EU (nutno ověřit u poskytovatele služby). Je tedy vhodné zvážit i otázky ochrany osobních údajů dle GDPR.
- Je nutné počítat s náklady spojenými s aktivací služeb a vyškolením odpovědného pracovníka.
- Základním předpokladem pro dobrou funkčnost cloudových služeb je kvalitní konektivita.
- Pokud se škola rozhodne využívat cloudové balíčky, tak je řádově snížen nárok na úložiště a správu serveru. Cloudový balíček může ulehčit online spolupráci v týmu a pomoci rozvíjet digitální gramotnost žáků a učitelů.
- Poskytovatel služeb musí splňovat nároky na ochranu osobních údajů dle GDPR.

6 Více viz <https://spomocnik.rvp.cz/clanek/22586/PLATFORMY-A-SYSTEMY-PRO-SKOLNI-KOMUNIKACI-A-SPOLUPRACI.html>

b) Vlastní serverové prostředí

- Data a informace školy jsou uloženy na serveru, který se fyzicky nachází v budově školy.
- O server se musí starat kompetentní personál, zejména je třeba zajistit:
 - Musí být umístěn na čistém, nejlépe bezprašném místě, kde se nebude přehřívat (nejlepší je klimatizovaná místnost).
 - Musí být uložen na bezpečném místě, ke kterému má přístup jen omezený počet lidí.
 - Pokud není umístěn v rozvaděči (racku), nesmí existovat překážky před ventilačními otvory.
 - Je doporučen minimálně jeden server pro doménový řadič⁷, který zvládne běh nejméně jednoho virtuálního stroje⁸ (virtualizován může být například email, školní informační systém apod.). Server musí mít minimálně dva zrcadlené disky.
 - Data serveru je nutné pravidelně zálohovat.
 - Doporučeno zvážit druhý záložní server pro případ vyřazení prvního serveru z provozu.

Technické požadavky

Minimální požadavek



V případě, že má škola správce, který zvládne pravidelně aktualizovat a spravovat koncová zařízení ručně, je možné v závislosti na charakteristice školy fungovat bez centrálního řízení účtů. Centrální řízení účtů je však doporučeno (viz výše).

- Pozn.: Ruční správa vyžaduje pravidelnou činnost na týdenní bázi v závislosti na charakteristice činnosti školy.

Standard konektivity škol



Parametr 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).

7 Doménový řadič (Active Directory) zajišťuje v počítačové síti autentizaci a autorizaci uživatelů, počítačů i další služby. Řadič domény výrazně ulehčuje administraci počítačové sítě. Dalo by se říci, že pro administrátora je při větším počtu koncových zařízení nezbytná, viz: https://cs.wikipedia.org/wiki/Active_Directory

8 Virtuální stroj je v informatice software, který vytváří virtualizované prostředí mezi platformou počítače a operačním systémem, ve kterém koncový uživatel může provozovat software na abstraktním stroji. Zjednodušeně řešeno, je to virtuální počítač běžící v jiném počítači (server). Virtuálních strojů může na serveru běžet více, záleží na tom, jak je server dimenzován. Virtualizované stroje se poté při poruchách jednodušeji přenášejí na jiné servery a virtualizace odděluje jednotlivé služby, ke kterým lze potom přistupovat jednotlivě a nastavovat pro každé jednoduše vlastní zabezpečení. Důležitá je také záloha virtuálních strojů.

- S** Parametr 2.2.2 Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém.

Doporučení nad rámec Standardu konektivity škol

- D** 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].
- D** Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele.
- D** Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací (např. aktivní zapojení do federovaného systému www.eduroam.cz)).
- D** Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 - IPFIX nebo ekvivalent).
- D** Zavedení více-faktorové autentizace.
- D** Podpora vzdáleného přístupu (VPN).
- D** Nástroje pro centrální správu a audit ICT prostředků.
- D** Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk aj.).
- D** Systémy pro monitorování funkčnosti síťové a serverové infrastruktury.
- D** Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management).

OBLAST 2: BEZPEČNÉ UKLÁDÁNÍ A SPRÁVA DAT ŠKOLY



Jak bylo řečeno, ve školním prostředí pracujeme často s citlivými daty, při jejichž zneužití hrozí až fatální následky a nemalé náklady. Podobnou hrozbou je ztráta těchto dat, a proto je potřeba je vždy zálohovat. Doporučuje se aplikovat pravidlo 3 – 2 – 1 (Vytvoření nejméně tří kopií dat – Uložení kopie na nejméně dva typy médií – Udržování alespoň jedné kopie zálohy mimo pracoviště).

Při práci s daty také musíme dodržovat platné zákony a nařízení, zejména týkající se ochrany osobních údajů, nebo vnitřní předpisy. Více informací k této problematice najdete v publikaci [Bezpečná digitální infrastruktura školy](#).

Co je třeba zařídit:

-  Bezpečné uložení dat žáků a zaměstnanců školy tak, aby nedošlo k jejich úniku nebo zneužití.
-  Uchovávání pouze takových dat, které je v souladu s pravidly pro ochranu osobních údajů dle GDPR.
-  Pravidelné zálohování výše uvedených dat.
-  Správné nastavení oprávnění pro čtení, ukládání a mazání dat na společných složkách/discích/prostředí.

Technické požadavky

Minimální požadavek

-  Záložní datové úložiště (NAS) je doporučeno, a to pro zálohování důležitých dat a souborů a pro uložení společných dat.
-  Základní datové úložiště se dvěma pevnými disky může být postačující (nutné konzultovat s odborníkem).
-  Je možné využít i univerzálních cloudových balíčků (viz výše), avšak s nastavením šifrovaného ukládání a oprávnění k přístupu/úpravě jen vybraným uživatelům.

Standard konektivity škol

-  Parametr 2.2.3 Systémy zálohování a obnovy dat serverové infrastruktury na externí úložiště (NAS).
-  Parametr 2.2.4 Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů.



OBLAST 3: PEVNÁ LAN – PŘIPOJENÍ KONCOVÝCH ZAŘÍZENÍ DO SÍTĚ ŠKOLY

Proč?

Zabezpečení koncových zařízení uživatelů (viz výše) je jen jedna stránka věci. Tato zařízení se musí bezpečně připojovat i do sítě tak, aby byla funkční a využitelná pro výuku i nepedagogickou práci. Práce s koncovými zařízeními nemá učitelé přidělovat potíže a starosti, ale má pomoci rozvíjet inženýrské myšlení a digitální kompetence žáků.

Pokud koncová zařízení nejsou do sítě zapojena správně, jednak nepomáhají vzdělávacím cílům a jednak může být ohroženo zařízení samotné, školní síť nebo i ostatní zařízení v síti.

Co je třeba zařídit:

- I** Funkční připojení koncových zařízení do sítě školy a vhodně je využívat ve výuce a při práci.

Technické požadavky

Minimální požadavek

- M** Aktivní prvek – switch s managementem⁹ - minimálně variantu 100/1000 Mb/s.
- M** Minimální konektivita koncových počítačových systémů 100/1000 Mb/s full duplex, ostatní systémy 100 Mbit/s.

Standard konektivity škol

- S** Parametr 2.3.1 Minimální konektivita koncových uživatelských zařízení 1000 Mb/s full duplex.
- S** Parametr 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.
- S** Parametr 2.3.3 Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3) 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.].
- S** Parametr 2.3.4 Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.).
- S** Parametr 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.

9 Switch – Síťový přepínač, častěji i v našem prostředí označovaný anglicky switch, je v informatice aktivní prvek v počítačové síti, který propojuje jednotlivé prvky do hvězdicové topologie. Přepínač obsahuje větší či menší množství síťových portů (až několik stovek), na něž se připojují síťová zařízení nebo části sítě. Jednoduše řečeno, switch je základní prvek počítačové sítě. Switche pracují na různých maximálních rychlostech 100 Mb/s, 1000 Mb/s, 10000 Mb/s a dále. V současné době bychom měli směřovat k tomu, aby port pro koncové zařízení měl rychlost 1000 Mb/s (1 Gb/s) a „páteřní trasy“ směřovat k 10000 Mb/s (10 Gb/s). Dále viz: https://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%BD_p%C5%99ep%C3%ADna%C4%8D. Přídomek „s managementem“ znamená možnost upravovat nastavení přepínače pomocí příkazové řádky nebo webového rozhraní (HTTP).

Doporučení nad rámec Standardu konektivity škol

- D** Propojení aktivních prvků a důležitých systémů (např. Servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku.



OBLAST 4: ŘEŠENÍ BEZDRÁTOVÝCH SÍTÍ (WLAN) – WI-FI

Proč?

V současnosti se většina zařízení připojuje k síti bezdrátově pomocí Wi-Fi. Připojování školních nebo vlastních přenosných zařízení (BYOD) je stále častější. K bezdrátové síti Wi-Fi se často mohou připojovat učitelé, žáci i návštěvníci a u všech skupin existuje riziko poškození celé sítě (například zavlčením viru), ať už úmyslně nebo neúmyslně. Zároveň musí být Wi-Fi síť spolehlivá, aby se mohl internet využívat pro vzdělávací cíle. Proto je nutné, aby každá skupina uživatelů měla svoji vlastní oddělenou Wi-Fi síť. Wi-Fi ve škole by měly být správně nastaveny a spravovány. V případě incidentu by měl být jeho původce dohledatelný. Dalším důležitým parametrem je odpovídající pokrytí a kapacita dle plánovaného počtu připojených zařízení. Před budováním Wi-Fi sítě tedy doporučujeme zpracování studie proveditelnosti ze strany potenciálního dodavatele¹⁰.

Co je třeba zařídit:

- I** Kvalitní a kontrolovaný přístup koncových zařízení do Wi-Fi sítě školy.
- I** Fyzická nepřístupnost některých zařízení (např. Wi-Fi router) běžným uživatelům.
- I** Dohledatelnost uživatelů v případě incidentu pomocí registrace.
- I** Dohledatelnost počítačových systémů v případě incidentu.
- I** Vytvoření více Wi-Fi sítí, tedy více SSID¹¹ (např. pro hosty, zaměstnance, žáky).
- I** Adekvátní nastavení přístupů pro skupinu uživatelů (např. žáci by neměli mít přístup do stejné Wi-Fi sítě jako pedagogové).
- I** Dostatečné pokrytí a kapacita Wi-Fi sítě dle plánovaného počtu zařízení. Sledování využití pokrytí a kapacity Wi-Fi sítě a reagování na případné přetížení sítě.

¹⁰ Roli při budování Wi-Fi sítě například hraje i síla zdíva.

¹¹ Název sítě Wi-Fi, neboli SSID (Service Set Identifier), je název, který vaše síť používá k oznamování své přítomnosti jiným zařízením. Více viz <https://cs.wikipedia.org/wiki/Wi-Fi>.

Návodné otázky

-  Kdo bezdrátovou síť Wi-Fi využívá a kde? Používá se i ve výuce?
-  Je povolen přístup na síť Wi-Fi i s vlastním zařízením?
-  K čemu by uživatelé Wi-Fi sítě ne/měli mít přístup?

Technické požadavky

Minimální požadavek

-  V případě, že je Wi-Fi využíváno pro zařízení učitelů a pro zařízení školy přidělené žákům. Každá skupina uživatelů má vlastní síť Wi-Fi, tedy SSID (název sítě).
-  Pokud je Wi-Fi používána i pro připojení soukromých zařízení žáků a dětí (tedy koncept BYOD), musí být síť Wi-Fi pro tato zařízení oddělena od školní sítě. Připojování zařízení je logováno¹².
-  Veškerý provoz u organizací spravovaných zařízení musí být zabezpečen minimálně AES šifrováním a standardem WPA2-Enterprise. Zabezpečení WPA2-PSK technologií se ve větších organizacích nedoporučuje; zabezpečení WEP technologií je nedostatečné.
-  Doporučená je centralizovaná správa Wi-Fi sítě¹³.

Standard konektivity škol

-  Parametr 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 žáků.
-  Parametr 2.4.2 Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu.
-  Parametr 2.4.3 Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky školy a externí zařízení (hosty).
-  Parametr 2.4.4 Podpora mechanismu izolace uživatelů.
-  Parametr 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.

¹² Je třeba zajistit logování (zaznamenání dat za účelem jejich analýzy), aby byl případný útočník-škoditel dohledán.

¹³ Centralizovaná správa wifi sítě – software/hardware, který umožní centrální správu všech wifi zařízení. Od základního nastavení po logování provozu a dohled nad wifi sítí.

Doporučení nad rámec Standardu konektivity škol

- D** Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokáce Wi-Fi v určitém čase.
- D** 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).
- D** Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací (např. aktivní zapojení do federovaného systému www.eduroam.cz).
- D** 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].

DALŠÍ ZDROJE INFORMACÍ

Bezpečná školní ICT infrastruktura – edukační videa. Edu.cz. Dostupné z:

<https://www.edu.cz/digitalizujeme/bezpecna-skolni-ict-infrastruktura/>

Bezpečnost – Systém podpory profesního rozvoje učitelů a ředitelů. Úvod - Systém podpory profesního rozvoje učitelů a ředitelů [online]. Dostupné z: <https://www.projektsypo.cz/bezpecnost>

KOPECKÝ, K., Základy počítačové bezpečnosti. Podpora kompetencí vedoucích pedagogických pracovníků při implementaci digitálních technologií do života školy/školského zařízení. [online]. Dostupné z: http://www.klus.upol.cz/wp-content/uploads/2021/02/pc_bezpecnost_kopecky.pdf

Bezpečná školní ICT infrastruktura (BEZIT). Edu.cz. Dostupné z <https://www.edu.cz/bezpecna-skolni-ict-infrastruktura-bezit-jako-prevence-pred-kybernetickou-kriminalitou/>.

Akademie CZ.NIC: <https://akademie.nic.cz/>

Osvětové materiály o kybernetické bezpečnosti a prevenci <https://osveta.nukib.cz/mod/page/view.php?id=1043>

Portál o digitalizaci škol: <https://edu.cz/digitalizujeme>

Příklad auditní zprávy k digitální infrastruktuře školy: <https://revize.edu.cz/files/auditni-zprava-2023-online.pdf>

PROKÁZÁNÍ A KONTROLA NAPLNĚNÍ STANDARDU KONEKTIVITY ŠKOL



MSMT
MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY

Praha, březen 2024

Č.j. MSMT-27467/2023-1

ÚVOD

Ministerstvo školství, mládeže a tělovýchovy (dále jen „MŠMT“) publikovalo Standard konektivity škol (dále také „Standard“), který je dostupný na webových stránkách <https://edu.cz/digitalizujeme>. Standard definoval základní technická kritéria cílového stavu školní síťové infrastruktury a přijatelnosti aktivit projektů naplňující požadavky na školy v 21. století, mj. i strategický cíl IROP 4.1 v oblasti zajištění vnitřní konektivity škol a připojení k internetu – rozvoj vnitřní konektivity v prostorách škol a školských zařízení a připojení k internetu¹.

Dokument *Prokázání a kontrola naplnění Standardu konektivity škol* je jednou ze tří metodických pomůcek pro školy, které mají za cíl pomoci jim se orientovat v problematice digitální infrastruktury školy. Jedná se o dokument pro všechny školy/příjemce, které mají prokázat naplnění parametrů uvedených ve Standardu. Je spíše technického rázu a slouží pro administrativní účely, proto je určen pro manažery projektů nebo správce/administrátory IT. U každého z parametrů Standardu je uvedeno, jakým způsobem by měl příjemce prokázat jeho naplnění. U parametrů, u kterých je to smysluplné, je uveden i způsob případného ověření na místě.

Nezapomeňte se na své cestě k digitalizaci školy podívat i na dva další metodické materiály a další zdroje z edu.cz/digitalizujeme:

- **Průvodce ke Standardu konektivity škol** blíže vysvětluje problematiku digitální infrastruktury školy, proč je potřeba ji kvalitně a funkčně zajistit a jak to udělat. Dokument je určen pro ředitele, ICT koordinátory, správce IT i zřizovatele. Dostupné na: <https://www.edu.cz/digitalizujeme/standard-konektivity-skol#pruvodce>
- **Bezpečná digitální infrastruktura školy** představuje základní principy, postupy a doporučení v oblasti kybernetické bezpečnosti pro školy. Dokument je určen především IT správcům či administrátorům. Dostupné na: <https://www.edu.cz/digitalizujeme/bezpecna-skolni-ict-infrastruktura/>
- **Bezpečná školní ICT infrastruktura** – edukační videa – dostupná na <https://www.edu.cz/digitalizujeme/bezpecna-skolni-ict-infrastruktura/>
- **IT správa** – Příručka ke správě ICT ve škole a příklady dobré praxe (rozhovory i videa) – dostupné na <https://www.edu.cz/digitalizujeme/it-sprava/>.

Nevíte, jak si Vaše škola stojí na poli digitální infrastruktury? Zda je dostatečná, funkční a bezpečná? Obraťte se na specializované IT guru, kteří Vám rádi pomohou a zdarma prověří stav digitální infrastruktury vaší školy. Více informací naleznete na <https://www.edu.cz/digitalizujeme/it-guru/>.

¹ Viz Programový dokument IROP 2021-2027 (<https://irop.mmr.cz/cs/irop-2021-2027/dokumenty>)

Další informace o metodické podpoře naleznete na
<https://www.edu.cz/digitalizujeme/metodicka-podpora/>.

V případě dotazů nás kontaktujte na digitalizujeme@msmt.cz.

Věříme, že Vám tento dokument a další metodická podpora poskytnutá MŠMT a Národním pedagogickým institutem ČR na cestě digitalizace Vaší školy pomůže a bude pro Vás inspirativní.

1. KONEKTIVITA ŠKOLY K VEŘEJNÉMU INTERNETU (WAN)

1.1. 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 parametry v době ukončení realizace a v průběhu udržitelnosti projektu.

1.2. POVINNÉ PARAMETRY PROJEKTU:

- 1.2.1.** Šíře pásma (bandwidth) odpovídající 0,25 Mbps/žák či student² nebo 0,5 Mbps/koncové uživatelské zařízení³ a zároveň taková šířka pásma, která neomezuje provoz zařízení a uživatelů⁵. Šíře pásma se vztahuje na počet žáků/studentů/koncových uživatelských zařízení v budově/areálu, kde se projekt realizuje.

Příklad: Určuje podle počtu žáků nebo podle počtu koncových zařízení. Např. pokud má škola 100 žáků a 40 koncových uživatelských zařízení, šířka pásma musí být buď 25 Mb/s (dle počtu žáků) nebo 20 Mb/s dle počtu koncových zařízení. V obou případech však platí, že šířka pásma neomezuje provoz zařízení a uživatelů.

Prokázání:

- Příjemce si ověří šíři pásma například nástrojem na webu www.standardkonektivity.cz⁶ a doloží export výsledku **nebo**
- příjemce doloží smlouvu s poskytovatelem konektivity, která musí být nastavena tak, aby poskytovaná šíře pásma neomezovala běžný školní provoz, příjemce doloží smlouvu **nebo**
- příjemce slovně popíše a vypočítá, že v rámci jeho parametrů (počet studentů/žáků, počet počítačů, počet zařízení přistupujících k internetu) dané připojení nijak neomezuje provoz zařízení a uživatelů.

2 Počet žáků/studentů je definovaný celkovým počtem žáků/studentů školy.

3 Koncové uživatelské zařízení je počítačový systém, který je aktivně využíván uživatelem (např. žákem, studentem nebo zaměstnancem školy) ke vzdělávacím či pracovním účelům (typicky počítač, notebook, tablet apod.).

4 Metrika vhodná typicky pro školy bez mobilních popř. BYOD zařízení

5 Definováno jako saturace šířky pásma připojení k veřejnému internetu, která ani ve špičkách nedosáhne, a to ani krátkodobě 100 %.

6 Další weby, na kterých lze šíři pásma ověřit, jsou: <https://speedtest.cesnet.cz/> či <https://netmetr.cz>.

1.2.2. Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy.

Prokázání:

- Příjemce ověří nástrojem na webu www.standardkonektivity.cz⁷ a doloží export výsledku **a zároveň**
- příjemce doloží smlouvu s poskytovatelem konektivity.

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.

Prokázání:

- Příjemce doloží nastavení logování požadovaných záznamů ze zařízení **a zároveň** popíše, jaký mechanismus logování používá (jak loguje a jak dlouho ukládá záznamy).

Ověření na místě:

- V případě prověření na místě bude přivolán technik a kontrolor ověří, že příjemce ukládá logy po deklarovanou dobu (namátkový záznam logu).

1.2.4. Síťové zařízení podporující rate limiting, antispoofing, access listy – zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality.

Prokázání:

- Příjemce slovně popíše potřebné komponenty a licence pro zajištění řádné funkcionality **a zároveň**
- příjemce doloží smlouvu, ze které bude patrná podpora rate limitingu, antispoofingu, access listy, **nebo**
- 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.

Prokázání

- Příjemce slovně popíše potřebné komponenty a licence pro zajištění řádné funkcionality **a zároveň**
- příjemce doloží smlouvu s dodavatelem, ze které bude patrná podpora požadované funkce **nebo**
- datasheet (produktový list) zařízení, ze kterého bude splnění parametru patrné.

⁷ Případně na <https://www.dnssec.cz/>

Příklad slovního popisu:

- V případě útoku, který detekuje firewall, router reaguje. Zdrojová IP adresa útočníka je vložena do Access listu útočníků. Ve firewallu je připraveno pravidlo, které všechny pokusy o přístup z adres útočníků blokuje.

- 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.).

Prokázání:

- Příjemce doloží nastavení domén ze svých systémů, ze které bude patrná podpora šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén **nebo**
- příjemce doloží smlouvu s poskytovatelem domén, ze které bude patrná podpora šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén **nebo**
- 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;

Prokázání:

- Příjemce ověří nástrojem na webu www.standardkonektivity.cz⁸ a doloží export výsledku **nebo**
- příjemce doloží smlouvu s poskytovatelem konektivity, ze které splnění parametru vyplývá.

Ověření na místě:

- Kontrolor se připojí zařízením do sítě a připojí se na stránky www.standardkonektivity.cz.

- 1.2.8.** Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici.

Prokázání:

- 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.

Ověření na místě:

- Kontrolor na místě ověří verzi softwaru vůči vydaným aktualizacím u výrobce.

⁸ Případně na stránce <https://www.dnssec.cz/>

- 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.

Prokázání

- Příjemce doloží smlouvu s poskytovatelem konektivity dokládající naplnění parametru **nebo**
- příjemce doloží prohlášení poskytovatele konektivity dokládající naplnění parametru.

1.3. DOPORUČENÉ PARAMETRY PROJEKTU:

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

- 1.3.1.** Symetrické připojení (zajištění konektivity) bez agregace a omezení, doporučujeme postupně směřovat ke kapacitě konektivity 1Gbps.

Prokázání:

- Příjemce splnění parametru ověří například nástrojem na webu www.standardkonektivity.cz⁹ a doloží export výsledku.

- 1.3.2.** Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách.

Prokázání:

- Příjemce ověří nástrojem na webu www.standardkonektivity.cz¹⁰ a doloží export výsledku **a zároveň**
- příjemce doloží smlouvu s poskytovatelem konektivity dokládající naplnění parametru společně s doprovodným XML otiskem databáze RIPE.

- 1.3.3.** Poskytovatel konektivity je schopen zajistit funkci systému incident response, monitoring a aktivní notifikaci anomálií síťového provozu, zamezení podvržení zdrojových IP adres (anti-spoofing), funkci pro blokování nežádoucí komunikace zahrnující nebo jinak omezující konektivitu a systémy školy pro zamezení zahlcení linky (např. RTBH, FlowSpec, služby AntiDDoS řešení), detekci a zamezení amplifikačních útoků, zabezpečení směrování síťového provozu pomocí RPKI a konfigurace odmítnutí nevalidních prefixů.

⁹ Další weby, na kterých lze šíři pásma ověřit, jsou: <https://speedtest.cesnet.cz/> či <https://netmetr.cz>.

¹⁰ Případně i <https://www.dnssec.cz/>

Prokázání:

- Příjemce doloží smlouvu s poskytovatelem konektivity dokládající naplnění parametru **nebo**
- příjemce doloží prohlášení poskytovatele konektivity dokládající naplnění parametru.

1.3.4. Antivirová kontrola internetového provozu.**Prokázání:**

- Příjemce doloží fakturu, licenci nebo datasheet (produktový list) zařízení zabezpečující antivirovou kontrolu internetového provozu a důkaz (např. printscreen) o aktivaci této funkcionality **nebo**
- příjemce doloží prohlášení poskytovatele konektivity dokládající naplnění parametru.

2. VNITŘNÍ KONEKTIVITA ŠKOLY (LAN A WLAN)

2.1. OBECNÝ POPIS

Vnitřní síťové prostředí školy pořizované v rámci projektu může být řešeno pevnou sítí, bezdrátovou sítí nebo kombinací těchto technologií. Připojení je nutné zajistit v prostorách dotčených hlavním projektem, rovněž je možné pokrýt ostatní prostory školy, včetně chodeb, jídelen, internátu a dalších školských zařízení. Potřebnost a účelnost takového pokrytí musí být odůvodněna ve studii proveditelnosti.

2.2. POVINNÉ PARAMETRY PROJEKTU (BEZ OHLEDU TYPU SÍŤOVÉHO PŘIPOJENÍ):

- 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).

Prokázání:

- 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) **nebo**
- příjemce doloží vnitřní předpis (např. směrnici) zajišťující naplnění parametru.

- 2.2.2.** Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém¹¹.

Prokázání:

- 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.

Ověření na místě:

- Kontrolor na místě ověří způsob logování do počítačového systému.
- Kontrolor na místě ověří, že příjemce ukládá logy po deklarovanou dobu (namátkový záznam logu).

¹¹ Počítačový systém je každý prvek informačních a komunikačních technologií využívající pro svoji činnost jak hardware, tak software. Pro účely standardů jsou rozlišována: 1. koncová uživatelská zařízení (např. osobní počítače, notebooky, tablety, mobily aj.) a 2. servery, síťové prvky, datová úložiště apod.

2.2.3. Systémy zálohování a obnovy dat serverové infrastruktury.

Prokázání:

- Příjemce popíše, jak je tento parametr naplněn (zejména popíše technologie a procesy pro zálohování a obnovu dat) **nebo**
- příjemce doloží vnitřní předpis (např. směrnici) zajišťující naplnění parametru.

2.2.4. Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů.

Prokázání:

- Příjemce doloží fakturu nebo čestné prohlášení dodavatele prokazující nákup služby pro antivirovou ochranu počítačových systémů a antispamovou ochranu poštovních serverů **a zároveň**
- 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.) **nebo**
- příjemce doloží vnitřní předpis (např. směrnici) zajišťující naplnění parametru.

2.3. POVINNÉ PARAMETRY PROJEKTU V OBLASTI PEVNÉ LAN:

2.3.1. Minimální konektivita koncových uživatelských zařízení 1000 Mbps full duplex.

Prokázání

- 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.

Prokázání

- 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.].

Prokázání

- 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) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru.

- 2.3.4.** Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.).

Prokázání

- 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) **nebo**
- příjemce doloží smlouvy/faktury od dovozce/ů, ze kterých bude zřejmé, jaká kategorie strukturované kabeláže byla použita, případně přiloží projekt.

- 2.3.5.** Páteří 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.

Prokázání

- 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) **nebo**
- příjemce doloží smlouvy/faktury od dodavatele/ů, ze kterých bude zřejmé, jaká kategorie strukturované kabeláže byla použita a jaký typ optického vlákna/metalického kabelu byl použit, případně přiloží projekt.

¹² 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 architekturu přepínacího subsystému.

2.4. MINIMÁLNÍ PARAMETRY PROJEKTU V PŘÍPADĚ ŘEŠENÍ BEZDRÁTOVÝCH SÍTÍ (WLAN):

- 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.

Prokázání

- Příjemce doloží smlouvy či jinou dokumentaci prokazující naplnění parametru (návrh topologie, projekt, dokumentace o měření apod. od dodavatele).

Ověření na místě:

- Příjemce ukáže fyzické rozmístění jednotlivých access pointů.

- 2.4.2.** Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu.

Prokázání

- Příjemce doloží datasheety (produktové listy) prokazující naplnění parametru **a zároveň**
- příjemce popíše, jak je tento parametr naplněn (zejména popíše konfiguraci centrálního managementu Wi-Fi sítě (security profile) a zda jsou aplikovány požadované parametry) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru.

- 2.4.3.** Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).

Prokázání

- Příjemce doloží vnitřní předpis (např. směrnici) zajišťující naplnění parametru **a zároveň**
- 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.) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění tohoto parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

Ověření na místě

- Kontrolor se na místě pokusí připojit k síti Wi-Fi příjemce jako host.

2.4.4. Podpora mechanismu izolace uživatelů.

Prokázání

- 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) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

Ověření na místě

- Příjemce namátkou provede izolaci uživatele, jeho zanesení na black list a následné odebrání uživatele z black listu.

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.

Prokázání

- Příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

2.5. DOPORUČENÉ PARAMETRY PROJEKTU (BEZ OHLEDU TYPU SÍŤOVÉHO PŘIPOJENÍ):

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

2.5.1. Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele.

Prokázání:

- Příjemce doloží nastavení logování požadovaných záznamů ze zařízení a popíše, jaký mechanismus logování používá (jak loguje a jak dlouho ukládá záznamy).

2.5.2. Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokace Wi-Fi v určitém čase.

Prokázání

- Příjemce doloží vnitřní předpis (např. směrnici) zajišťující naplnění parametru **a zároveň**
- příjemce popíše, jak je tento parametr naplněn (zejména popíše, jak jsou dočasné přístupy poskytovány, jak dochází k jejich odebrání, jak je nastaven systém blokace Wi-Fi apod.) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktový list) prokazující naplnění parametru.

- 2.5.3.** Federované služby autentizace a autorizace, včetně aktivního zapojení do národních vzdělávacích federací (např. aktivní zapojení do federovaného systému www.eduroam.cz).

Prokázání:

- Příjemce doloží potvrzení od CESNET pomocí exportu výsledků z webu <https://pripojovani.eduroam.cz/>.

- 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 spravované access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení).

Prokázání

- 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].

Prokázání

- 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) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktový list) prokazující naplnění parametru.

Ověření na místě:

- Kontrolor se pokusí připojit k Wi-Fi síti příjemce (dojde k ověření certifikátu nebo jména a hesla)

- 2.5.6.** Propojení aktivních prvků a důležitých systémů (např. servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku.

Prokázání

- Příjemce doloží datasheety (produktový list) prokazující naplnění parametru.

3. DALŠÍ DOPORUČENÉ BEZPEČNOSTNÍ PRVKY PROJEKTU

Nad rámec povinných parametrů uvedených v bodech 1 a 2 je dále doporučeno v projektu realizovat:

- 3.1.1.** Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 – IPFIX nebo ekvivalent).

Prokázání

- Příjemce popíše, jak je tento parametr naplněn (zejména popíše, jaké systémy nebo zařízení jsou využívány), **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

- 3.1.2.** Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie.

Prokázání

- Příjemce popíše, jak je tento parametr naplněn (zejména popíše, jaké systémy jsou využívány), **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

- 3.1.3.** Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management).

Prokázání

- Příjemce popíše, jak je tento parametr naplněn (zejména popíše, jaké systémy jsou využívány), **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

- 3.1.4.** Systémy pro monitorování funkčnosti síťové a serverové infrastruktury.

Prokázání

- Příjemce popíše, jak je tento parametr naplněn (zejména popíše, jaké systémy jsou využívány) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

- 3.1.5.** Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatelů (učitel, žák), blokování nežádoucích kategorií obsahu.

Prokázání

- Příjemce popíše, jak je tento parametr naplněn (zejména popíše, jaká zařízení jsou využívána) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

- 3.1.6.** Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk aj.).

Prokázání

- Příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží prohlášení poskytovatele prokazující naplnění parametru.

- 3.1.7.** Nástroje pro centrální správu a audit ICT prostředků.

Prokázání

- Příjemce popíše, jak je tento parametr naplněn (zejména jaké nástroje pro centrální správu a audit ICT prostředků jsou využívány) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

- 3.1.8.** Podpora vzdáleného přístupu (VPN).

Prokázání

- Příjemce popíše, jak je tento parametr naplněn a **zároveň**
- příjemce doloží smlouvy **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

- 3.1.9.** Zavedení více-faktorové autentizace.

Prokázání

- Příjemce popíše, jak je tento parametr naplněn **nebo**
- příjemce doloží smlouvy, faktury nebo licence prokazující splnění parametru **nebo**
- příjemce doloží datasheety prokazující naplnění parametru (záznam nastavení zařízení, výpis z operačního logu řešení).

Ověření na místě:

- Kontrolor se pokusí připojit k systémům vyžadující více-faktorovou autentizaci