Střední škola André Citroëna Boskovice

TECHNICKÁ ZPRÁVA

Akce:	Modernizace výuky technických oborů a vnitřní konektivity na Střední škole André Citroëna Boskovice, Integrovaného regionálního operačního programu pod č. CZ.06.4.59/0.0/0.0/16_075/0011327
Část:	Zasíťování školy - slaboproudé rozvody
Číslo akce:	5/2019
Stupeň:	DPS - Dokumentace provedení stavby
Vypracoval:	[redacted]
Datum:	01/2020

OBSAH:

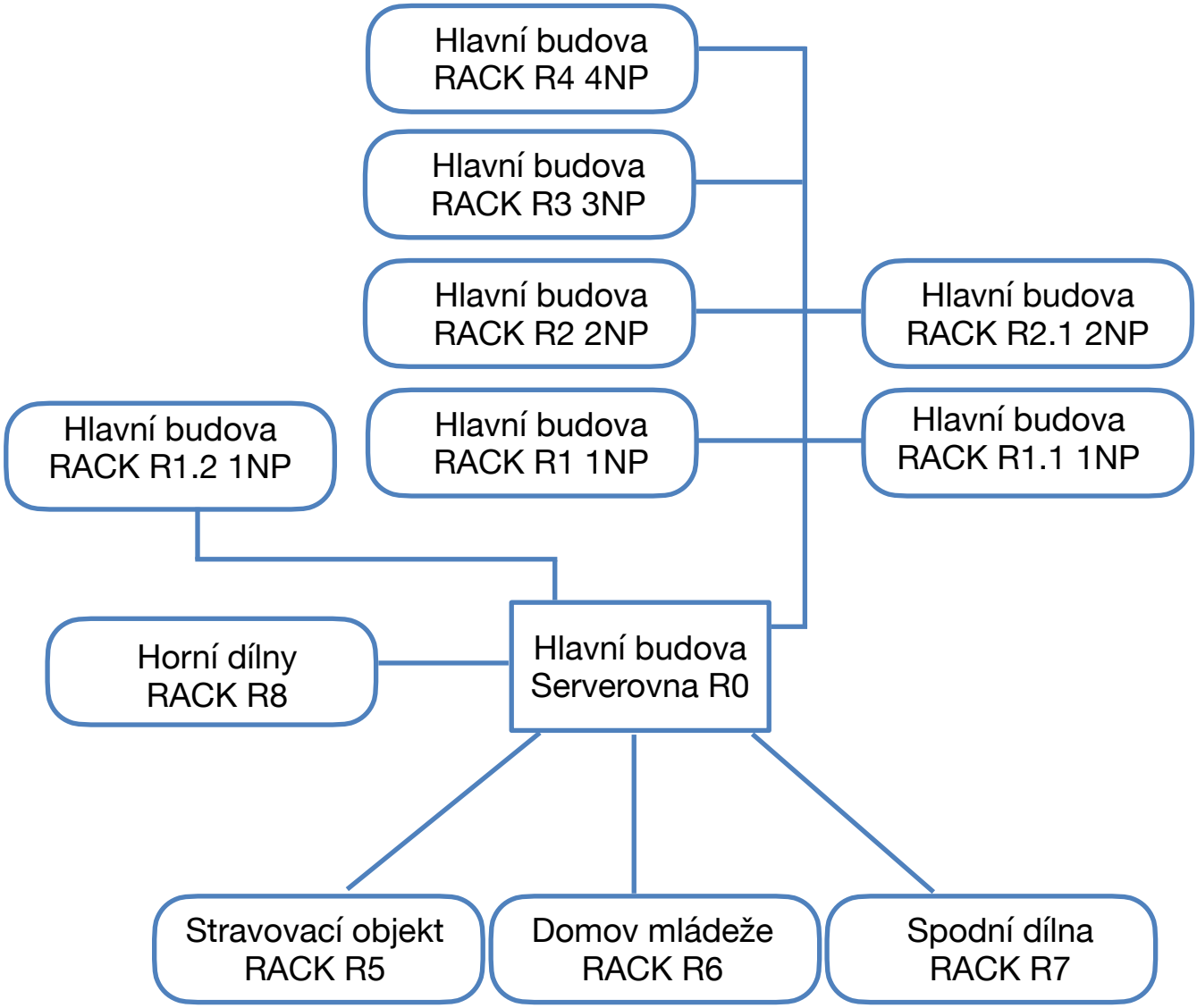
1. Řešení projektu

1.1. Rozsah projektovaného zařízení

1.1.1. Technická zpráva řeší

- Pasivní prvky sítě (dle výkresové dokumentace)
- Silnoproudé rozvody navázané na pasivní prvky sítě (dle výkresové dokumentace)

Pasivní prvky sítě jsou rozděleny na páteřní rozvody a rozvody v jednotlivých částech budov.
Páteřní rozvody jsou řešeny pomocí optických kabelů.
Rozvody v jednotlivých částech jsou zajištěny metalickým vedením cat6a.



1.2. Identifikace stavby

Název stavby:	Střední škola André Citroena Boskovice, nám.9.května 2153/2a, 680 01 Boskovice
Charakter stavby:	Modernizace výuky technických oborů a vnitřní konektivity na Střední škole André Citroëna Boskovice, Integrovaného regionálního operačního programu pod č. CZ.06.4.59/0.0/0.0/16_075/0011327
Investor:	Střední škola André Citroena Boskovice, nám.9.května 2153/2a, 680 01 Boskovice
Stupeň dokumentace:	Dokumentace pro realizaci
Projektant elektro:	
Zpracováno:	leden 2020

1.3. Základní normy a předpisy

Projektová dokumentace je zpracována dle platných technických předpisů, norem, katalogů výrobců a návodů pro montáž jednotlivých zařízení, platných v době zpracování projektové dokumentace. Dále projekt respektuje všechny náležitosti dle oborových zvyklostí, zásady směrnic a požadavky investora dle Metodik, PNE a ČSN, zejména:

- ČSN 33 0120 /IEC 93/ - Elektrotechnické předpisy - Normalizovaná napětí IEC
- ČSN 33 0165 /EN 60446/ - Elektrotechnické předpisy. Značení vodičů barvami nebo číslicemi. Prováděcí ustanovení
- ČSN 33 1500 - Elektrotechnické předpisy. Revize elektrických zařízení
- ČSN 33 2000-1 - Elektrické instalace budov Část 1: Rozsah platnosti, účel a základní hlediska
- ČSN 33 2000-1 ed.2 - Elektrické instalace nízkého napětí Č ást 1: Základní hlediska, stanovení základních charakteristik, definice
- ČSN 33 2000-4-41 ed.2 - Elektrické instalace nízkého napětí

Část 4-41: Ochranná opatření pro zajištění bezpečnosti - Ochrana před úrazem elektrickým proudem

- ČSN 33 2000-4-42 - Elektrotechnické předpisy. Elektrická zařízení.

Část 4: Bezpečnost. Kapitola 42: Ochrana před účinky tepla

- ČSN 33 2000-4-43 ed.2 - Elektrické instalace nízkého napětí

Část 4-43: Bezpečnost - Ochrana před nadproudy

- ČSN 33 2000-4-47 - Elektrotechnické předpisy Elektrická zařízení

Část 4: Bezpečnost - Kapitola 47: Použití ochranných opatření pro zajištění bezpečnosti
Oddíl 470: Všeobecně - Oddíl 471: Opatření k zajištění ochrany před úrazem elektrickým proudem

- ČSN 33 2000-4-473 - Elektrotechnické předpisy. Elektrická zařízení.

Část 4: Bezpečnost. Kapitola 47: Použití ochranných opatření pro zajištění bezpečnosti. Oddíl 473: Opatření k ochraně proti nadproudům

- ČSN 33 2000-4-481 - Elektrotechnické předpisy Elektrická zařízení

Část 4: Bezpečnost - Kapitola 48: Výběr ochranných opatření podle vnějších vlivů -
Oddíl 481: Výběr opatření na ochranu před úrazem elektrickým proudem podle vnějších vlivů

- ČSN 33 2000-4-482 - Elektrotechnické předpisy Elektrická zařízení

Část 4: Bezpečnost - Kapitola 48: Výběr ochranných opatření podle vnějších vlivů - Oddíl 482: Ochrana proti požáru v prostorách se zvláštním rizikem nebo nebezpečím

- ČSN 33 2000-5-51 ed.3 - Elektrické instalace nízkého napětí

Část 5-51: Výběr a stavba elektrických zařízení - Všeobecné předpisy

- ČSN 33 2000-5-523 ed.2 - Elektrické instalace budov
Část 5: Výběr a stavba elektrických zařízení - Oddíl 523: Dovolené proudy v elektrických rozvodech

- ČSN 33 2000-5-53 - Elektrotechnické předpisy. Elektrická zařízení.
Část 5: Výběr a stavba elektrických zařízení. Kapitola 53: Spínací a řídicí přístroje

- ČSN 33 2000-5-54 ed.2 - Elektrické instalace nízkého napětí
Část 5-54: Výběr a stavba elektrických zařízení - Uzemnění, ochranné vodiče a vodiče ochranného pospojování

- ČSN 33 2000-5-56 ed.2 - Elektrické instalace nízkého napětí
Část 5-56: Výběr a stavba elektrických zařízení - Zařízení pro bezpečnostní účely

- ČSN 33 2000-7-701 ed.2 - Elektrické instalace nízkého napětí
Část 7-701: Zařízení jednoúčelová a ve zvláštních objektech - Prostory s vanou nebo sprchou

- ČSN 33 2030 - Elektrostatika - Směrnice pro vyloučení nebezpečí od statické elektřiny

- ČSN 33 2130 ed.2 - Elektrické instalace nízkého napětí - Vnitřní elektrické rozvody

- ČSN 33 3051 - Ochrany elektrických strojů a rozvodných zařízení

- ČSN 33 3210 - Elektrotechnické předpisy. Rozvodná zařízení. Společná ustanovení

- ČSN 33 4010 - Elektrotechnické předpisy.
Ochrana sdělovacích vedení a zařízení proti přepětí a nadproudu atmosférického původu

- ČSN 38 0810 - Použití ochran před přepětím v silových zařízeních

- ČSN 73 0802 - Požární bezpečnost staveb - Nevýrobní objekty

- ČSN 73 0804 - Požární bezpečnost staveb - Výrobní objekty

- ČSN 73 0818 - Požární bezpečnost staveb - Obsazení objektů osobami

- ČSN 73 0831 - Požární bezpečnost staveb - Shromažďovací prostory

- ČSN 73 6005 - Prostorové uspořádání sítí technického vybavení

- ČSN 74 3282 - Ocelové žebříky. Základní ustanovení

- ČSN EN 1838 - Světlo a osvětlení – Nouzové osvětlení

- ČSN EN 12464-1 - Světlo a osvětlení
Osvětlení pracovních prostorů - Část 1: Vnitřní pracovní prostory

- ČSN EN 50172 - Systémy nouzového únikového osvětlení

- ČSN EN 50266 - Společné zkušební metody pro kabely za podmínek požáru
Zkouška vertikálního šíření plamene na vertikálně namontovaných svazcích vodičů nebo kabelů

- ČSN EN 50266-2-2 - Společné zkušební metody pro kabely za podmínek požáru
Zkouška vertikálního šíření plamene na vertikálně namontovaných svazcích vodičů nebo kabelů – Část 2-2: Postupy - Kategorie A

- ČSN EN 60059 - Normalizované hodnoty proudů IEC

- ČSN EN 60445 ed.4 - Základní a bezpečnostní zásady pro rozhraní člověk-stroj, značení a identifikaci - Identifikace svorek předmětů, konců vodičů a vodičů

- ČSN EN 60529 - Stupně ochrany krytem (krytí - IP kód

- ČSN EN 60664-1 ed.2 - Koordinace izolace zařízení nízkého napětí
Část 1: Zásady, požadavky a zkoušky

- ČSN EN 60909-0 (33 3022) - Zkratové proudy v trojfázových střídavých soustavách
Část 0: Výpočet proudů

- ČSN EN 62305 – 4 ed.2 - Ochrana před bleskem
Část 4: Elektrické a elektronické systémy ve stavbách

- ČSN IEC 1200-52 - Pokyn pro elektrické instalace
Část 52: Výběr a stavba elektrických zařízení - Výběr soustav a způsoby kladení vedení

- ČSN IEC 60331 - Zkoušky elektrických kabelů za podmínek požáru - Celistvost obvodu

- ČSN EN 50174-2 ed.2 - Informační technologie - Instalace kabelových rozvodů
Část 2: Projektová příprava a výstavba v budovách

- Vyhláška 50/78 Sb.

1.4. Katalogy výrobců a dodavatelů

- výrobce/dodavatel kabelů
- výrobce/dodavatel jistících prvků a přístrojů, rozvodnic
- výrobce/dodavatel úložných plastových systémů
- výrobce/dodavatel úložných drátěných a kovových systémů
- výrobce/dodavatel pasivních prvků

2. Základní technické údaje

2.1. Provozní údaje pro jednotlivé prostory

Určení vnějších vlivů dle ČSN 33 2000-1 ed.2 a ČSN 33 2000-5-51 ed.3:

Vnitřní prostory objektu – provozní místnosti (vyjma umývacích prostor a prostor s vanou nebo sprchou), kanceláře, učebny, sklady, chodby, schodiště:
přiřazení vnějších vlivů z hlediska nebezpečí úrazu elektrickým proudem - prostory normální

Vnitřní prostory objektu – umývací prostory a prostory s vanou nebo sprchou:
přiřazení vnějších vlivů z hlediska nebezpečí úrazu elektrickým proudem - prostory zvlášť nebezpečné zóny dle ČSN 33 2000-7-701 ed.2

Vnitřní prostory objektu – prostory technického zázemí:
přiřazení vnějších vlivů z hlediska nebezpečí úrazu elektrickým proudem - prostory nebezpečné

Venkovní prostory objektu :
přiřazení vnějších vlivů z hlediska nebezpečí úrazu elektrickým proudem - prostory zvlášť nebezpečné V souladu s vyhláškou č. 499/2006 Sb. je provedeno určení vnějších vlivů odbornou komisí

Napěťové soustavy

hlavní obvody:	3 NPE ~ 50Hz, 400V / TN-C-S
pomocné obvody:	1 NPE ~ 50Hz, 230V / TN-S
	3 NPE ~ 50Hz, 400V / TN-S

2.2. Ochrana před úrazem elektrickým proudem

Návrh je řešen v souladu s ČSN EN 61140 ed. 2 (EN 61140) a jeho základním pravidlem, že nebezpečné živé části nesmí být přístupné a přístupné vodivé části nesmí být nebezpečně živé ani za normálních podmínek, ani za podmínek jedné poruchy.
Ochrana za normálních podmínek je zajištěna základní ochranou a ochrana za podmínek jedné poruchy je zajištěna ochranou při poruše.
Prostředky zvýšené ochrany zajišťují ochranu za obou podmínek.
Dále je pak ochrana před úrazem elektrickým proudem řešena v závislosti na druhu instalace nebo sítě v souladu s ČSN 33 2000-4-41 ed.2 (pro instalace NN).

2.3. Použité ochranné opatření

2.3.1. Základní ochrana (Ochrana před nebezpečným dotykem živých částí)

Základní ochrana elektrického zařízení, (před nebezpečným dotykem živých částí) je dána jejich provedením a konstrukčním uspořádáním a je řešena některým z následujících ochranných prostředků dle výše uvedených norem:

- Ochrana izolací živých částí
- Ochrana kryty nebo přepážkami
- Ochrana zábranou

- Ochrana doplňkovou izolací (prostředek zvýšené ochrany)

2.3.2.Ochrana při poruše (Ochrana před nebezpečným dotykem neživých částí)

Ochrana před neb. dotykem živých částí v napěťové soustavě 3NPE ~ 50Hz, 400V / TN-C-S
Izolací dle ČSN 33 2000-4-41 ed.2
Krytím dle ČSN 33 2000-4-41 ed.2
Doplňková proudovým chráničem dle ČSN 33 2000-4-41 ed.2
Ochrana malým napětím SELV dle ČSN 33 2000-7-702 ed.2

Základní
-automatickým odpojením od zdroje dle ČSN 33 2000-4-41 ed.2
-uzemněním dle ČSN 33 2000-4-41 ed.2
-pospojováním dle ČSN 33 2000-4-41 ed.2

Zvýšená
-doplňujícím pospojováním dle ČSN 33 2000-4-41 ed.2
-proudovým chráničem
-ochrana malým napětím SELV dle ČSN 33 2000-7-702 ed.2

2.3.3.Ochrana proti zkratu a přetížení

V soustavě 3 NPE ~ 50Hz, 400V / TN-C-S budou osazeny jističe nebo pojistky s odpovídající charakteristikou pro bezpečné vypnutí příslušné části elektrického zařízení.

2.3.4.Ochrana proti účinkům SEMP

Bude realizovaná dle požadavků.
Ochrana proti účinkům přepětí musí splňovat podmínky ČSN EN 60664-1.

2.3.5.Ochrana proti účinkům LEMP

-vnější ochrana bleskosvodová instalace (ZBO 0)
-vnitřní ochrana vyrovnáním potenciálů s použitím svodičů přepětí (ZBP O/E)

2.3.6.Stupeň důležitosti dodávky el.energie

Dodávka el. energie pro běžný provoz bude provedena ve stupni 3 ze sítě NN, bez nároku na zvláštní opatření.

2.4. Měření el.energie

2.4.1.Fakturační měření el.energie

Není dotčeno, TZ neřeší.

2.4.2.energetická bilance

Není dotčeno, TZ neřeší.

2.5. Vnější vlivy a prostory

Projektová dokumentace řeší výběr a instalaci elektrického zařízení při určeném způsobu provozu tak, aby byly zajištěny základní podmínky bezpečnosti dle ČSN 33 2000-5-51 ed. 3 a PNE 33 0000-2 ed. 4 na základě působení okolí (prostředí) na elektrické zařízení a naopak.
Přítomnost vnějších vlivů v jednotlivých prostorech předurčuje míru nebezpečí úrazu elektrickým proudem nebo elektrickým či elektromagnetickým polem. Na základě příslušného prostředí v jednotlivých prostorech jsou určena příslušná krytí a provedení jednotlivých elektrických zařízení dle požadavků na bezpečnost, (osoby, zvířata, majetek).
Uvedený protokol nebyl provozovatelem předložen, pro účely zpracování PD jsou uvažovány vnější vlivy v příloze "Protokol o určení vnějších vlivů".

2.6. Provedení uzemňovací soustavy

Není dotčeno, TZ neřeší.

2.7. Provedení ochrany před bleskem

Není dotčeno, TZ neřeší.

2.8. Ochrana před účinky atmosférického a průmyslového přepětí

Vnitřní ochrana před účinky atmosférického a průmyslového přepětí je navržena ve třech stupních:

1.stupeň ochrany před účinky atmosférického přepětí bude osazen svodiči bleskových proudů typu „B/C" instalovanými v hlavním rozvaděči objektu.

2.stupeň ochrany před účinky atmosférického přepětí bude osazen svodiči bleskových proudů typu „C" instalovanými v podružných rozvaděčích objektu.

3.stupeň ochrany před účinky atmosférického přepětí bude osazen svodiči bleskových proudů typu „D" instalovanými v zásuvkách 230V v racku – "zásuvková lišta".

Podmínkou účinnosti ochrany proti přepětí je její kompletnost, tj. svodiči bleskových proudů musí být ošetřeny všechny kabely vstupující ze zóny 0 do zóny 1 a být splněny podmínky pro pospojování a uzemnění. Při umístění přepěťových ochran je nutno dodržet minimální předepsané vzdálenosti mezi jednotlivými stupni ochran, nebo se musí mezi jednotlivé stupně vřadit oddělovací impedance. Podmínkou pro správnou funkci přepěťových ochran je kvalitní spojení svodičů se zemí.

2.9. Technické řešení

2.9.1.Demontáže stávajících rozvodů a zařízení

Veškeré stávající rozvody budou demontovány a ekologicky zlikvidovány dle zákona č.185/2001. Jedná se o plastové vkládací lišty pro vedení kabeláže, kabely UTP cat5e, rozvodnice “rack”.
Aktivní prvky, které nebudou již využity budou ekologicky zlikvidovány dle zákona č.185/2001, oddíl 8, §37f-37s.

2.9.2.Montáže nových rozvodů a zařízení

Navržená koncepce spočívá ve vytvoření páteřních rozvodů pomocí optických kabelů mezi jednotlivými datovými rozvodnicemi. Skříňová rozvodnice R0 bude umístěna v serverovně v 1PP a odtud budou provedeny jednotlivé propoje do podružných racků optickými kabely, které budou vedeny stoupacím vedením a rozvody v plastových lištách.

Propoj se stravovací budovou do racku R5 bude proveden ve spojovacím krku budovy, nad sádrokartonovým stropem v instalační plastové trubce. Projekt počítá s možností protažení stávající trasou. V případě, že budou zjištěny překážky, bude demontován sádrokartonový strop a trasa připravena nově.

Propoj s budovou “Domov mládeže” do racku R6 bude proveden ve stávajícím propoji v zemi. Projekt počítá s možností protažení stávající trasou. V případě, že budou zjištěny překážky, bude nutné konzultovat s investorem zřízení nové trasy.

Propoj s budovou “Horní dílny” do racku R8 bude proveden ve stávajícím propoji v zemi. Projekt počítá s možností protažení stávající trasou. V případě, že budou zjištěny překážky, bude nutné konzultovat s investorem zřízení nové trasy.

Propoj s budovou “Spodní dílna” do racku R7 bude proveden nově propojem v zemi. Optický kabel bude uložen v chráničce v pískovém loži min. 80 cm hlubokém. Napojení optického kabelu bude provedeno z datového rozváděče R0 v horních dílnách.

Podružné datové rozvodnice v jednotlivých patrech hlavní budovy budou propojeny optickými kabely vedenými stoupacím vedením v plastových chráničkách z hlavní datové rozvodnice R0, která bude umístěná v 1PP v serverovně.

Všechny podružné datové rozvodnice budou napájeny nově zřízeným kabelem CYKY-J 3x2,5mm2, který bude jištěn v nejbližším stávajícím rozváděči NN. V rozváděčích NN budou provedeny úpravy pro osazení nového proudového chrániče s jističem 16/1N/003 (charakteristika “B”, 10kA) a svodiče bleskových proudů typu „C“.
V hlavním rozváděči NN RMS1 bude osazen svodičem bleskových proudů typu „B/C“.
Současně s přívodním kabelem bude přiveden zž vodič CYA 4mm2 pro doplňující pospojování.

V u čebně 122 bude instalována nová datová rozvodnice R1.1 pro připojení datových zásuvek učeben IT č. 121 a 122. Přívod bude optickým kabelem z datové rozvodnice R0.

V učebně č.103 bude stávající datová rozvodnice zachována, bude označena R1.2. Přívod bude optickým kabelem z datové rozvodnice R0.

V učebně č.201 bude instalována nová datová rozvodnice, bude označena R2.1. Přívod bude optickým kabelem z datové rozvodnice R0.

Rozvody jednotlivých přípojných míst v hlavní budově budou vedeny z jednotlivých podružných datových rozvodnic v jednotlivých patrech ve vkládacích plastových lištách.

Metalické rozvody jsou provedeny kabely Cat6a a ukončeny ve dvojzásuvkách RJ45 Cat6a přisazenými na zdi. Přístupové body pro AP budou ukončeny v jednozásuvkách RJ45 Cat6a.

Přístupové body AP v ostatních budovách školy budou připojeny kabelem Cat5e a ukončeny v patřičném podružném datovém rozváděči v budově.

V hlavní budově bude v šatně 1PP instalována jedna zásuvka RJ45 pro připojení AP (access point).

V hlavní budově budou na chodbě 1NP instalovány 4ks zásuvek RJ45 pro připojení AP (access point).

V hlavní budově budou na chodbě 2NP instalovány 4ks zásuvek RJ45 pro připojení AP (access point), v učebně č. 222 bude instalována jedna zásuvka RJ45 pro připojení AP.

V hlavní budově budou na chodbě 3NP instalovány 4ks zásuvek RJ45 pro připojení AP (access point).
V hlavní budově budou na chodbě 4NP instalovány 4ks zásuvek RJ45 pro připojení AP (access point).

V budově “Domov mládeže” bude instalováno 7ks zásuvek RJ45 pro připojení AP (access point).

V budově “Horní dílny” bude instalováno 7ks zásuvek RJ45 pro připojení AP (access point).

V budově “Spodní dílny” bude instalováno 2ks zásuvek RJ45 pro připojení AP (access point).

V budově “Jídelna, svařovna, tělocvična” bude instalováno 4ks zásuvek RJ45 pro připojení AP (access point).

V areálu dílen Dřevařská je konektivita již vyřešena, bude pouze provedena výměna stávajících 4ks AP za nový typ, z důvodu centrální správy celého systému školy.

V hlavní budově školy jsou instalovány 2ks venkovních IP kamer, které jsou napojeny do datového rozváděče, který bude zrušen, proto je potřeba tyto kamery přepojit do nově instalovaného datového rozváděče.

Po provedené montáži bude provedeno měření s vystavením protokolu o měření jednotlivých okruhů.

Upozornění
Trasy, počty a rozmístění jednotlivých prvků budou upřesněny investorem před započetím realizace dle aktuálních požadavků a podmínek.

Doplňující ochranné pospojování
Hlavní datová rozvodnice R0 bude uvedena na stejný potenciál propojením zž vodičů CYA 4mm2 z ekvipotenciální svorkovnice EPS. Svorkovnice EPS bude připojena na hlavní PE sběrnu v HR vodičem CYA 4mm2.
Každá podružná datová rozvodnice Rx bude propojena zž CYA 4mm2 se sběrnou PE v patřičném podružném rozváděči NN.

3. Bezpečnost a ochrana zdraví při práci

Veškeré montážní práce musí být prováděny dle platných bezpečnostních předpisů, nařízení a platných norem. Před započetím prací musí být pracovníci náležitě poučeni a vybaveni patřičnými pracovními pomůckami a ochrannými pracovními prostředky. V průběhu montáže je nutno dodržovat veškeré zásady bezpečnosti práce a hlavně při práci ve výškách.
Montáž bude ukončena nutnými měřeními, dílčími revizemi a závěrečnou revizí a vypracováním celkové výchozí revizní zprávy.

Důležité upozornění
Jakékoliv další montáže zařízení nebo zásahy do hromosvodní soustavy musí provádět pouze osoba nebo firma, která je dostatečně kvalifikovaná a seznámená s novou normou ČSN EN 62305.

4. Požadavky na ostatní profese

Předmětem této dokumentace není prostorová koordinace s ostatními profesemi.

5. EMC

Podle zákona o technických požadavcích na výrobky č.22/1997 Sb. a nařízení vlády č.169/1997 Sb. musí být přístroje včetně vybavení a instalací provedeny a namontovány tak, aby elektromagnetické rušení, které způsobují, nepřesáhlo povolenou úroveň a naopak musí mít odpovídající odolnost vůči vystavenému elektromagnetickému rušení, která jim umožňuje provoz v souladu se zamýšleným účelem.
Přepětí, případně jiné rušivé impulsy, negativně ovlivňují funkci všech elektrických zařízení. Zařízení mohou být přepětím i zničena. Proto je nutno dle uvedeného zákona a dle Č SN 33 2000-1 odst.131.6.2, ČSN 33 4010, ČSN 33 2030, ČSN EN 60664-1 a ČSN 38 0810 provést taková opatření, která co nejvíce vlivy přepětí potlačí.
Při prostupu stavebními konstrukcemi musí být zaručen odstup mezi trasami slaboproudých a silnoproudých rozvodů minimálně 150 mm.

6. Základní požadavky pro montáž a uvedení zařízení do provozu

Montáž zařízení smí provádět pouze firma, která má pro tuto činnost vyškolený personál. Kromě toho musí být pracovníci dodavatelských firem prokazatelně vyškoleni výrobcem příslušného zařízení a musí mít osvědčení o oprávnění zařízení montovat či provádět na něm servis. Při instalaci musí pracovníci dodavatelských firem bezpodmínečně dodržovat všechna právní ustanovení, týkající se bezpečnosti práce a ochrany zdraví pracovníků. Montáž musí odpovídat příslušným technickým podmínkám výrobců. Zařízení smí být připojena na napájecí elektrickou síť a uzemnění teprve po provedení řádné revize. Revizní zpráva o stavu elektrického napájení a přívodu nesmí být po lhůtě, dané výše citovanou technickou normou.
Provozní zkoušky zařízení slouží k ověření nastavení dodaného systému, ověřují jeho funkčnost a zároveň prokazují splnění požadovaných kvalitativních ukazatelů předmětné dodávky. Sjednání podmínek zkoušek bude zajištěno smlouvou mezi odběratelem a dodavatelem. Námi předkládaná dokumentace neřeší ani program předepsaných zkoušek, ani jejich náplň.
Před uvedením jednotlivých zařízení do provozu bude zajištěno přezkoušení celého systému. Podle dohody sjednané s odběratelem může být na dohodnutou dobu sjednán i zkušební provoz zařízení. O případných provozních zkouškách bude sepsán zápis, který se stane nedílnou součástí předávací dokumentace. Součástí přejímacího zápisu bude komplexní dokumentace skutečného provedení.

Před předáním zařízení do užívání je třeba zajistit vyškolení jeho obsluhy a především by měla být uzavřena servisní smlouva o technické údržbě zařízení po skončení záruční lhůty.

6.1. Revize el. zařízení

Výchozí revizi provede dodavatel montážních prací podle ČSN 33 1500. Další revize periodické provede provozovatel ve stanovených lhůtách a po každé opravě vyvolané poruchou či poškozením el. zařízení dílčí revize.

6.2. Výstražné tabulky a nápisy

El. zařízení, popř. předměty musí být před uvedením do provozu vybaveny bezpečnostními tabulkami a nápisy předepsanými pro tato zařízení příslušnými zařizovacími nebo předmětovými normami.

7. Závěr

Při všech pracech (stavebních, elektro, montáž technologie) musí být dodržovány platné předpisy OBP. Výstavba veškerých rozvodů a zařízení nemá vliv na stávající životní prostředí. Zařízení není zdrojem nebezpečného záření ani jiných zdraví škodlivých produktů. Elektrická zařízení lze uvést do provozu jen po vykonání výchozí revize s kladným výsledkem. Při souběhu se silovými rozvody musí být ponechána odstupová vzdálenost dle ČSN 34 2300. Elektrická zařízení se musí pravidelnou údržbou a prohlídkami udržovat v bezpečném a provozuschopném stavu. Servis zařízení provádí výrobce nebo organizace jim pověřená, které má pro tuto činnost prokazatelně vyškolené osoby a je vybavena potřebným zařízením a materiálem. Pravidelné revize el.zařízení se provádějí dle ČSN 331500.

PROTOKOL
o určení vnějších vlivů vypracovaný odbornou komisí dle ČSN 33 2000-5-51 ed.3

Složení komise:
předseda:

členové:

Název objektu: Střední škola André Citroena Boskovice, nám.9.května 2153/2a, 680 01 Boskovice

Podklady použité pro vypracování protokolu:
TZ - "Modernizace výuky technických oborů a vnitřní konektivity na Střední škole André Citroëna Boskovice, Integrovaného regionálního operačního programu pod č.
CZ.06.4.59/0.0/0.0/16_075/0011327"

Popis objektu: Učebny, kancelářské prostory, soc. zázemí (šatny, WC, sprchy, ...), technické zázemí a komunikační prostory, venkovní prostory

Rozhodnutí:
Ve všech vnitřních prostorech, mimo místnosti níže uvedené, jsou vnější vlivy následující (prostory normální):
Prostředí - AA5, AB5, AC1, AD1, AE1, AF1, AG1, AH1, AK1, AL1, AM1, AN1, AP1, AQ1, AR1, AS1 Využití – BA2, BC1, BD1, BE1
Konstrukce budovy - CA1, CB1
V místnostech se sprchami je výskyt vody - AD3 (zóny dle ČSN 33 2000-7-701 edice 2), ostatní vnější vlivy zůstávají stejné (viz výše)
Kuchyně - (prostory nebezpečné):
Prostředí - AA5, AB5, AC1, AD2, AE1, AF1, AG1, AH1, AK1, AL1, AM1, AN1, AP1, AQ1, AR1, AS1 Využití – BA2, BC1, BD1, BE1
Konstrukce budovy - CA1, CB1
Ve venkovních prostorech jsou vnější vlivy následující (prostory zvlášť nebezpečné):
Prostředí - AA7, AB8, AC1, AD3, AE4, AF2, AG1, AH1, AK1, AL1, AM1, AN1, AP1, AQ1, AR1, AS1 Využití – BA2, BC3, BD1, BE1
Konstrukce budovy - CA1, CB1.

Zdůvodnění:
Vnější vlivy byly určeny v souladu s ČSN 33 2000-3, ČSN 33 2000-5-51 ed.3.

Datum sepsání protokolu: 27.1.2020

.....
podpis předsedy komise

Rozvaděč	Aktivní prvek
RO (serverovna)	CORE 24port SFP+
	CORE 24port SFP+
R1 (hlavní)	L3 48port SFP+ PoE
	L3 48port SFP+ PoE
R1.1 (IT1 121+122)	48port SFP+
R2	L3 48port SFP+ PoE
	L3 48port SFP+ PoE
R2.1 (IT2 201)	48port SFP+
R3	L3 48port SFP+ PoE
R4	L3 48port SFP+ PoE

R5 (údržba - stravování, tělocvična)	24port SFP+ PoE

R6 (domov mládeže)	48port SFP+
	48port SFP+
	24port SFP+ PoE

R7 (spodní dílny)	24port SFP+ PoE

R8 (horní dílny, sklad)	24port SFP+ PoE
	48port SFP+

R8.1 (220)	48port SFP+ PoE

TECHNICKÁ SPECIFIKACE / projekt - část - Konektivita

Střední škola André Citroëna Boskovice,
příspěvková organizace
náměstí 9. května 2153/2a,
680 11 Boskovice
IČO: 00056324
DIČ: CZ00056324 (plátce DPH)

TECHNICKÁ SPECIFIKACE

Základní požadavky na technické řešení

(1) Cílem projektu je zvýšení bezpečnosti a související modernizace IT infrastruktury, aby implementací projektu byly naplněny Standardy konektivity škol [1] - uvedené v příloze č.1 (dále jen Standard konektivity). Dílčí cíle dle jednotlivých komodit jsou specifikovány následovně:

Označení	Komodita	Počet
K1	Virtualizační platforma - serverová infrastruktura	1
K2	Zabezpečení LAN a Wifi – sítová infrastruktura	1
K3	Centrální logování	1

(2) Je požadováno řešení zachovávající a rozvíjející současné softwarové platformy Microsoft pro zachování kompatibility se stávajícími systémy a aplikacemi. Přechod na jinou platformu by způsobil uživatelské a provozní potíže.

(3) Pokud dodavatel vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k realizaci zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.

(4) Pokud dodavatelem nabízené řešení vyžaduje komponenty či služby neobsažené v požadavcích zadání, zahrne dodavatel do své ceny všechny náklady na jejich pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu, přičemž nesmí překročit předpokládanou hodnotu zakázky.

(5) Veškerá dokumentace vytvořená v rámci realizace veřejné zakázky, musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, Open Office, PDF) používaných zadavatelem. Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena zadavatelem.

1. TECHNICKÁ SPECIFIKACE – Konektivita

1.1. Specifické požadavky na technické řešení

(1) **K1 - Virtualizační platforma**

(a) Celé řešení je postaveno na třech fyzických serverech pro serverovou virtualizaci, které jsou napřímo připojeny ke sdílenému dvouřadičovému diskovému poli. Typ připojení diskového pole je SAS. Díky tomu je maximální počet k poli připojitelných serverů 4 (to odpovídá maximálnímu počtu portů na každém řadiči diskového pole). Networking vrstva je řešena dvěma ethernet CORE přepínači.

(b) Backup prostředí je řešen stávajícím vyhrazeným fyzickým serverem s VM a NAS diskovým polem připojeným do LAN včetně UPS. NAS a UPS budou součástí dodávky.

(c) Všechna propojení (jak k diskovému poli, tak do CORE switchů) jsou řešena redundantně.

(d) Vysoká dostupnost je zajištěna na úrovni serverů a CORE networkingu, ne na úrovni diskového pole a neCORE switchů.

(e) Součástí je i dodávka licencí operačních systémů a přístupových licencí s neomezeným počtem virtuálních serverů v licenčním programu pro EDU.

(f) výpadek jednoho fyzického serveru znamená nutnost využití HA funkcí Hyper-V, případně ruční zásah. VM, které běžely na porouchaném nebo z důvodu maintenance odstavovaném serveru, je třeba nastartovat na druhém fyzickém serveru. Servery mají dostatek procesorového výkonu a paměti na běh veškerých(případně vybraných) VM. Výpadek v poskytování služeb DC je pouze na dobu restartu VM

(g) výpadek jednoho ethernetového switche nezpůsobí výpadek v poskytování služeb DC

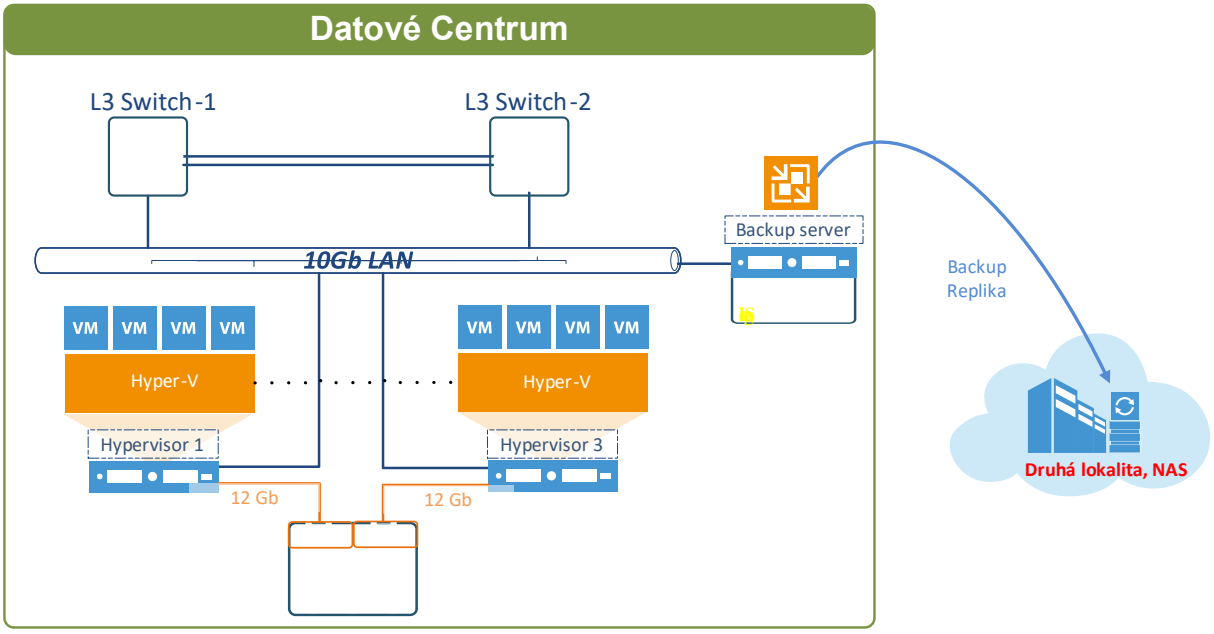
(h) výpadek jednoho řadiče diskového pole nezpůsobí výpadek v poskytování služeb DC

(i) výpadek celého diskového pole způsobí výpadek v poskytování služeb DC

(j) Provozní zabezpečení bude tvořeno souborem non-IT technologií, které zajistí optimální podmínky pro spolehlivý chod technologií – především serveru:

(i) Záložní zdroj napájení UPS zajistí chod serveru při výpadku napájení

(k) Pro zajištění bezpečnosti a možnosti řízení provozu v síti a zajištění prokazatelného monitoringu, logování a auditu interního i externího síťového provozu bude vybudována centrální databáze identit na bázi adresářové služby. Adresářová služby umožní ukládání a přehlednou správu identit (účtů včetně metadat) učitelů, žáků i externích subjektů, ale i technických prostředků – serverů, tiskáren, pracovních stanic apod. Adresářová služba bude poskytovat službu LDAP a umožní snadné napojení autentizačních mechanismů a protokolů – radius, agenta firewallu a dalších. Adresářová služba zajistí ověřování uživatelů pro účely jejich autorizace k přístupu k síťovým prostředkům (LAN, Internet atd.) i výpočetním zdrojům (pracovní stanice, tiskárny, sdílené složky atd.). Technické provedení bude založeno min. na 1 řadiči adresářové služby. Řadič bude provozován a bude pravidelně automaticky zálohovány. Součástí řadičů budou základní síťové služby – DNS, DHCP.


Datové Centrum
L3 Switch-1
L3 Switch-2
10Gb LAN
Backup server
Backup
Replika
VM
VM
VM
VM
Hyper-V
Hypervisor 1
12 Gb
VM
VM
VM
VM
Hyper-V
Hypervisor 3
12 Gb
Druhá lokalita, NAS

(2) **K2- Zabezpečení LAN a Wifi**

(a) Bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby s využitím technologie 802.1X.

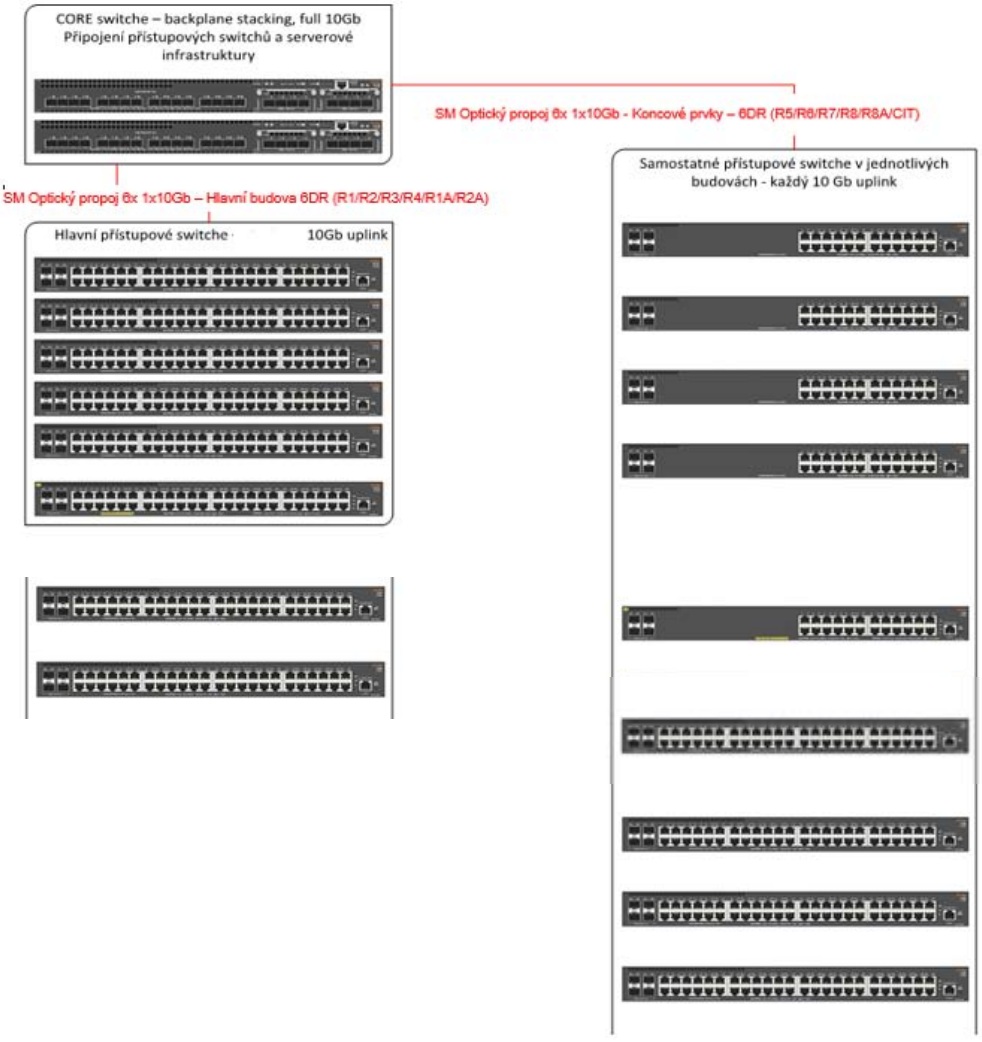
(b) Řízení provozu v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s routováním (přepínáním) provozu mezi VLAN na úrovni centrálního přepínače s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (QualityofServices).

(c) Architektura WiFi bude založena na řešení s centrální správou prováděnou virtuálním kontrolerem (řadičem), který bude součástí firmwarů přístupových bodů.

(d) Ověřování přístupu do WiFi sítě bude realizováno na stejném principu jako LAN (tj. protokol 802.1X + radius). Wifi bude nabízet více SSID (učitelé, žáci, Guest), které budou obsluhovány samostatnými VLAN a budou napojeny na raduis servery. Učitelé a žáci budou prostřednictvím radius serveru ověřováni v adresářové služby. Zabezpečení vnitřních sítí (BSSID) školy bude provedeno dle 802.1i, tedy - WPA2 s AES šifrováním a konfigurováno shodně pro obě frekvenční pásma. Výjimkou bude síť určená výhradně pro hosty (GuestWiFi).

(e) LAN Infrastruktura se skládá

- 2x CORE switche 24x 1000/10000 SFP+ portů (STACK)
- Hlavní přístupové switche – uplink 10Gb - Hlavní budova 6DR (R1/R2/R3/R4/R1A/R2A) – celkem 8KS aktivních prvků – rozložení dle přílohy: Rozvaděče
- Samostatné přístupové switche v jednotlivých budovách – uplink 10Gb - Koncové prvky – 6DR (R5/R6/R7/R8/R8A/CIT) – celkem 9KS aktivních prvků - rozložení dle přílohy: Rozvaděče
- LAN infrastruktura bude až ke koncovým aktivním prvkům v rychlostech 10Gb – koncové stanice budou připojeny rychlostí 1Gb



(3) **K3 - Centrální logování**

(a) Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací - může jednat o jediné zařízení, softwarový nástroj či appliance. Řešení umožní správu z jedné grafické konzole, přístupné nativně skrze https bez nutnosti instalace klienta. Data bude ukládána do jedné databáze (nebo více integrovaných databází) tak, aby bylo možno realizovat multikriteriální vyhledávání napříč informacemi z různých zdrojů (např. přepínače/ netflow a firewall/syslog).

(b) Veškeré dále požadované informace si bude systém automaticky získávat, vyčítat z monitorovaných systémů a současně bude umožňovat příjem protokolů určených pro přenos logovacích, provozních informací, alertů a událostí. Systém bude přijímat informace standardními protokoly ze síťových a dalších aktivních zařízení a Windows server systémů.

(c) Mandatorní informace, která bude v systému vždy obsažena a uchována, je vazba IP-uživatel-čas. Tuto informaci bude systém čerpat ze securityevent-logu adresářové služby, dále z informací o probíhajících komunikacích prostřednictvím firewallu a dalších přístupových a autentifikačních systémů (např. radius logy). Dále budou získávány informace o překladu zdrojových, vnitřních IP adres na externím výstupním rozhraní firewallu, kde bude prováděn NAT. Bude se tedy jednat o informace obsažené v NAT tabulce. Spolu s tím musí být po stanovenou dobu možné zpětně dohledat i vnější provoz k vnitřnímu zařízení. Další funkcionalitou bude plnohodnotná práce se síťovými toky, jejich zpracování a archivace. Nástroje systému budou umožňovat i analytickou práci s přijímanými toky a to i zpětně.

1.2. Implementační služby

(1) V rámci implementace předmětu plnění dodavatel realizuje pro všechny nabízené komodity K1 až K3

(a) Dodávka a implementace předmětu plnění musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií. Musí být v souladu s nabídkou uchazeče a se Standardem konektivity.

(b) Zajištění projektového vedení realizace předmětu plnění.

(c) Provedení testů.

(d) Předání do plného provozu.

(2) Zadavatel dále požaduje provést minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Dodavatel je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

K1: Virtualizační platforma
a) Návrh a kompletní implementace serverové virtualizační platformy b) Implementace pořízených technologií c) Návrh vhodné struktury ActiveDirectory, její vybudování d) Implementace automatické odstávky a najetí serveru v případě výpadku a obnovení dodávky elektrické energie e) Implementace zálohovacího SW včetně metodiky zálohování a obnovy dat f) Návrh a provedení akceptačních testů
K2: Zabezpečení LAN a Wifi
a) Implementace pořízených technologií b) Provedení segmentace LAN – VLAN, adresování, routování c) Zavedení IPv6 pro přístup k internetovým zdrojům publikovaným na IPv6 adresách d) Návrh a implementace 802.1X pro kabelovou LAN i WiFi včetně uživatelské dokumentace pro konfigurace obvyklých zařízení a jejich systémů - PC, notebooky, chytré telefony, tablety, tiskárny - Windows, Linux, MacOS, Android, IOS, embedded systémy periferií e) Návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro školu f) Vybudování VPN pro vzdálený přístup uživatelů LAN g) Respektování min. 3 různých skupinu uživatelů (učitelé, studenti, hosté) v návrzích a implementaci bezpečnostních a ostatních politik h) Zajištění ostatních nezbytných činností pro naplnění Standardu konektivity
K3: Centrální logování
a) Návrh a implementace systému pro centrální logování pro naplnění požadavků Standardu konektivity, především, ale nejen: • logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel, a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.) b) Provedení souvisejících konfigurací monitorovaných systémů

(3) Akceptační testy musí pro všechny komodity vždy zahrnovat minimálně prokázání kompletnosti dodávky a požadované funkčnosti. Povinným akceptačním kritériem bude prokázání naplnění požadavků Standardu konektivity dle manuálu uveřejněného na http://www.strukturalni-

fondy.cz/cs/Microsites/IROP/Novinky/Zverejneni-doporucujiciho-manualu-k-postupum-pri-prokazani-a-kontrole včetně úspěšného provedení a doložení testu na https://www.standardkonektivity.cz/. Prokázání naplnění požadavků poskytne dodavatel v písemné formě vhodné jako příloha k Závěrečné zprávě o realizaci projektu.

1.3. Školení

(1) Školení bude pokrývat všechna zařízení a systémy všech komodit, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu:

(a) běžných administrátorských činností pro implementované systémy

(b) standardní údržby systémů pro administrátory zadavatele

(2) Školení dále zajistí seznámení pracovníků zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.

(3) Minimální rozsah školení pro každou komoditu je 1MD, není-li uvedeno jinak. Školení bude probíhat v sídle zadavatele.

1.4. Harmonogram projektu

(1) Zadavatel vyžaduje dodržení následujícího maximálního harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky. Údaj D značí datum podpisu smlouvy o dílo. Čísla značí počet kalendářních dnů.

Aktivita	Začátek	Termín
Podpis smlouvy	D	D
Zahájení projektu – úvodní projektová schůzka	D	D+7
Realizace předmětu plnění	D+7	D+47
Školení administrátorů	D+47	D+48
Akceptační testy	D+48	D+50
Zahájení ostrého provozu	D+60	-

(2) Dodavatel může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.

(3) Dodavatel uvede závazný harmonogram plnění ve své nabídce a zároveň v návrhu smlouvy.

1.5. Popis povinných parametrů dodávaného řešení

(1) V dále uvedených tabulkách jsou uvedeny povinné parametry prvků nabízeného řešení. Dodavatel musí všechny parametry splnit, v případě nesplnění požadavku zadavatele bude nabídka dodavatele vyřazena a dodavatel bude následně vyloučen z účasti v zadávacím řízení.

(2) Dodavatel ve své nabídce uvede značkové specifikace nabízených dodávek. Z popis způsobu naplnění bude možno určit, že nabízené řešení jednoznačně splňuje všechny aspekty povinného parametru.

Povinné parametry pro Komoditu K1 - Virtualizační platforma:

Parametr	
Formát serveru	Rackové provedení, min.. 1U, Pro přístup ke všem komponentám serveru není nutné nářadí. Barevně značené hot-plug vnitřní i vnější komponenty
CPU	Server musí být osazen 2x CPU, minimálně s osmi procesorovými jádry. Hodnocení výkonu nabídnutého serveru musí být publikované na webu: https://www.cpubenchmark.net s minimálními parametry: • Passmark CPU Mark, hodnota min: 22 000 /CPU
RAM	128GB v provedení min. DDR4, min. 2933 MHz
Diskový subsystém	Server musí být osazen min. dvěma pevnými disky s kapacitou alespoň 480GB SSD
Optická mechanika	Není požadována.
Síťové rozhraní + napájení	• 1x Broadcom 57412 2 Port 10Gb SFP+ + 5720 2 Port 1Gb Base-T, rNDC • 1x Broadcom 57412 Dual Port 10Gb, SFP+, PCIe Adapter, Low Profile • 1x SAS 12Gbps HBA External Controller, LP Adapter • Redundance napájení
Podpora a servis	Podpora na 24 měsíců typu NBD, oprava v místě instalace serveru

Diskové pole	Diskové pole SAS (12Gb SAS 8 Port Dual Controller) musí být osazeno: 2x 960GB SSD SAS Read Intensive 12Gbps 512 2.5in Hot-plug 16x 1.8TB HDD 10K 512e SAS12 2.5
Podpora a servis	Podpora na 24měsíců typu NBD, oprava v místě instalace serveru do 4hodin od nahlášení

SW licence operačních systémů	Serverové operační systémy	3 ks licencí 64-bitového serverového operačního systému v aktuální verzi. Licence musí umožnit provoz neomezeného počtu virtuálních serverů stejné verze v prostředí nabízené serverové virtualizace, dále provoz všech nabízených aplikací a management nástrojů.
	Klientské licence	klientské licence pro nabízené operační systémy umožňující využívat těchto systémů uživatelům je celkem 600 (user CAL).

SW licence zálohování	BACKUP SW	Zálohovací SW pro EDU pokrývající 3NODY (6CPU) – umožňující granulární obnovy
	Klientské licence	Záruka 24měsíců

UPS **1x**	Kapacita výstupního výkonu [W]: 4 500 Kapacita výstupního výkonu [VA]: 5 000 Jmenovité výstupní napětí [V]: 200/208/220/230/240V Topologie: Dvojitá on-line konverze se systémem PFC (korekce účiníku) Výstupní přípojky: -(8) IEC-320-C13 -(2) IEC-320-C19 -(1) Hardwired
	- KOMUNIKACE A SPRÁVA - Port rozhraní: 1 adaptér NMC, 1 USB port, 1 port RS232 (port USB a RS232 nemohou být použity současně), 4 bezpotenciálové kontakty (DB9), 1 miniaturní svorkovnice se svorkami pro dálkový start a odstavení, 1 svorkovnice pro dálkové vypnutí, 1 konektor DB15 pro paralelní chod - Ovládací panel: Vícejazyčný LCD displej
	Záruka: min. 24 měsíců

NAS **1x**	CPU min: 2400 bodu v CPU Benchmarks na https://www.cpubenchmark.net/ RAM 4GB, paměť rozšiřitelná až na: 64 GB (16 GB x 4 GB)
	- Šachta(y) pevného disku: 16 - Maximální počet šachet pevného disku s rozšiřující jednotkou: 28 - Kompatibilní typ disku: 3.5" SATA HDD, 2.5" SATA HDD, 2.5" SATA SSD - Maximální interní hrubá kapacita: 192 TB (12 TB drive x 16) - Maximální hrubá kapacita s rozšiřovacími jednotkami: 336 TB (192 TB + 12 TB drive x 12) - Maximální velikost jednoho svazku: 108 TB - Disky vyměnitelné za provozu: Ano - Min 2x 10Gb port - Ližiny do racku - Min. 4x 8T HDD (disk určený pro provoz v NAS)
	Záruka: min. 24 měsíců

Povinné parametry pro Komoditu K2 – Zabezpečení LAN a Wifi:

Firewall **1KS**
22 x GE RJ45 ports (including 2 x WAN ports, 1 x DMZ port, 1 x Mgmt port, 2 x HA ports, 16 x switch ports with 4 SFP port shared media), 4 SFP ports, 2x 10G SFP+, 480GB onboard storage, dual power supplies redundancy. Max managed APs (Total / Tunnel) 128 / 64 Minimální parametry výkonu: Propustnost FW min. 18Gbps NGFW propustnost 1,4 Gbps Firewall musí obsahovat: IPS, Malware Protection, Application Control, Web Filtering, Antispam, Data Leak Prevention.
Záruka min. 24 měsíců v režimu 24x7.

Centrální přepínač 2x	
	- Management: Fully managed - Layer 3 Advanced: L2 switching / L3 Static routing / RIP routing / Multicast routing / OSPF - 24x 1000/10000 SFP+ port portů (možno 16portu + 8portu in slot) - podpora až 8x SFP+ portů nebo 2x 40GbE port s volitelným modulem - Redundantní zdroje - Možnost stohování - Montáž do 19“ racku. Úchytky jsou součástí balení. - Správa sítě a zabezpečení za pomoci nástorjů výrobce - Modulární 10GbE a 40GbE uplink pro bezdrátovou agregaci
	- 4-port module to allow stacking + kabel 1m
	Záruka: min. 24 měsíců, odeslání náhradního zařízení max. následující pracovní den po nahlášení závady

Přístupové přepínače 17KS	**Společné parametry**	
	Základní parametry	L3 přepínač v rackovém provedení max. 1U – 6KS L2 přepínač v rackovém provedení max. 1U – 11KS
	Stohování	podpora stohování pro jednotný management (přepínače musí stohovatelné vzájemně bez ohledu na provedení - viz. Porty a propustnost)
	Propustnost	neblokovaná architektura
	Agregace portů	podpora LACP
	Dualstack	IPv4 a IPv6 dualstack včetně podpory ACL a QoS
	VLAN	VLAN 802.1Q, MAC i protocolbased, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření
	Ověřování uživatelů a zařízení	podpora 802.1X
	Monitoring a správa	plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní
	Záruka	min. 24 měsíců, odeslání náhradního zařízení max. následující pracovní den po nahlášení závady
	Specifické parametry	
	Porty a propustnost	**L3 switch 6 kus** – 48x 1 GB RJ-45 PoE + 4x SFP+ (nesdílené), min. 170 Gb/s **5 kusů** – 48x 1 GB RJ-45 + 4x SFP+ (nesdílené), min. 150 Gb/s **1 kusů** – 24x 1 GB RJ-45 + 4x SFP+ (nesdílené), min. 100 Gb/s **4 kusy** – 24x 1 GB RJ-45 PoE + 4x SFP+ (nesdílené), min. 100 Gb/s **1 kus** – 48x 1 GB RJ-45 PoE + 4x SFP+ (nesdílené), min. 170 Gb/s
WiFi přístupové body (AP) + montáž na strop 42KS – INDOOR	Základní funkce	Přístupový bod (AP) WiFi včetně montážního materiálu na stěnu nebo strop
	Frekvence	činnost v radiovém pásmu 2,4 a 5 GHz současně, 2 radiové moduly
	Anténní systém	interní systém min. MIMO 3x3 (5 GHz) a MIMO 2x2 (2,4 GHz), optimalizovaný pro montáž na strop
	Přenosové rychlosti	SU-MIMO (5GHz) až 1300Mbps, MU-MIMO až 867Mbps. 2,4GHz MIMO až 300Mbps.
	Standardy	podpora 802.3at, 802.11n, 802.11ac, 802.1x včetně přiřazování do VLAN
	Řízení klientů	automatické směrování komunikace klientů z 2.4 GHz na 5 GHz (pokud klienti podporují obě pásma)
	Rušení	průběžná detekce non-WiFi rušení a spektrální analýza
	Multi SSID	podpora vysílání min. 8 SSID (WiFi sítí) současně, podpora přiřazení každého SSID samostatné VLAN
	Zatížení	min. 250 přiřazených (asociovaných) klientů na radiový modul
	Porty	min. 1x 1Gb, PoE s podporou standardů 802.3at a 802.3af
	Úsporné napájení	podpora standardu 802.3az - Energy-EfficientEthernet (EEE)
	Řízení provozu	klasifikace a kontrola provozu, detekce obvyklých aplikací s možností určení priority nebo šířky pásma zvoleného provozu
	Řízení kvality služeb	automatické řízení kvality služeb (QoS) pro hlas a video
	Současná obsluha více klientů	Podpora MU-MIMO (Multi-User MIMO) - multi-user multiple input/multiple output
	Přenosové rychlosti	SU-MIMO (Single-User MIMO) min. 1300Mb, MU-MIMO min. 850 Mb

	Bezpečnost	Detekce cizích přístupových bodů zjištěných v LAN i v radiofrekvenčním pásmu
	Virtuální kontroler	Virtuální, vysoce dostupný kontroler obsažený ve firmware každého přístupového bodu. Umožňuje kompletní centrální správu WiFi infrastruktury a řízení jejího provozu včetně roamingu klientů.
	Monitoring a správa	plná podpora CLI, SSH, SNMP 1-3, syslog, web rozhraní
	Správa frekvenčního pásma	automatické dynamické přidělování kanálů a řízení výkonu přístupových bodů pro vyrovnané pokrytí a minimalizaci interference
	Záruka	min. 24 měsíců

Minigbic + DAC	Základní funkce	34x 10G SFP+ LC LR 10km 6x 10G SFP+ to SFP+ 3m DAC Cable

Povinné parametry pro Komoditu K3 – Centrální logování:

Monitorovací a logovací systém 1x	Základní funkce	Systém pro sběr, ukládání a správu provozních a bezpečnostních informací a událostí ze sledovaných systémů
	Protokoly sběru logů	syslog, TCP, UDP, HTTP, AMQP, JSON
	Sběr síťových toků	netflow či kompatibilní dle nabízeného firewallu a centrálního přepínače
	Zdroje logů	Min. REST API, textové soubory, Radius, ActiveDirectory, MS SQL databáze, Windows Event Log - včetně rozšířených "Applications and ServicesLogs", síťové prvky - syslog a netflow, ostatní aktivní prvky - syslog, SNMP trap
	Parsování logů	Integrovaný nástroj pro parsování logů. Možnost nahrání části logu, online vytváření parseru a snadné testování výsledku. Podpora vytváření opakovaně použitelných vzorků - např. definice IP adresy regulárním dotazem apod.
	Retence	Uchovávání logů min. 6 měsíců, automatická retence logů a indexů
	Geolokace	Podpora automatické doplňování logů o informaci o lokalitě podle IP adresy
	Normalizace logů	Sjednocení názvů shodných dat z různých zdrojů logů např. pro snadné vyhledávání napříč zdroji
	Rozšíření logů	Podpora rozšíření logů o vlastní statické a dynamické (kalkulované) položky integrovaným nástrojem.
	Rozšiřitelnost	Podpora snadného rozšíření funkčnosti pomocí plug-inů nebo modulů
	Bezpečnost	Podpora šifrované komunikace se zdroji (SSL apod.), ověřování zdrojů (TLS apod.)
	Výkon	Min. 500 EPS (event per second), 5000 FPM (flows per minute)
	Dashboardy	Uživatelské vytváření dashboardů (pracovních desek) včetně možnosti využití grafických prvků (grafy, mapy, histogramy apod.) i strukturovaných dat (tabulek)
	Export dat	Export dat do csv a/nebo xls - min. výsledky hledání
	Kanály	Možnost vytváření kanálů - datových sad či toků - na základě pravidel (logických podmínek) a to i napříč různými zdroji. Podpora dalšího zpracování - tvorba alarmů, zobrazení na dashboardu, online odesílání do nadřazeného systému apod.
	Alerty, notifikace	Podpora vytváření alertů - překročení okamžitých či kumulovaných hodnot, zasílání upozornění
	ActiveDirectory	integrace s ActiveDirectory pro ověřování uživatelů, nastavení oprávnění min. administrátor a operátor
	Vyhledávání	Rychlé a intuitivní vyhledávání v záznamech napříč všemi zdroji i při velkých objemech dat (řády TB). Jednoduchý dotazovací jazyk. Rychlá vyhledávání či filtrování bez tvorby dotazů - např. výběrem v kontextovém menu vybraného pole uloženého záznamu.
	Kompatibilita	Podpora provozu v prostředí nabízené serverové virtualizace
	Ukládání dat	do databáze, případná databázová licence musí být součástí dodávky

	Výstupy	Možnost výstupů do nadřazeného systému pro účely vzdáleného expertního dohledu. Zabezpečený přenos vhodným protokolem
	Záruka	min. 24 měsíců včetně poskytnutí opravných verzí

Příloha č.1

STANDARD KONEKTIVITY ŠKOL

1. Konektivita školy k veřejnému internetu (WAN)

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

- šíře pásma (bandwidth) odpovídající 128kbps/student[2] nebo 512kbps/počítač[3] nebo taková šířka pásma, která neomezuje provoz zařízení a uživatelů[4]
- vlastní nebo poskytovatelem přidělené veřejné IPv4 i IPv6 adresy
- plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack)
- validující DNSSEC resolver na straně školy
- podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení
- logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)
- síťové zařízení podporující ratelimiting, antispoofing, ACL/xACL, rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality
- zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu, antivirovou kontrolou stahovaného obsahu
- možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků
- podpora DNSSEC a IPv6 protokolů pro služby školy dostupné online
- u software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po celou dobu udržitelnosti projektu.

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

- symetrické připojení bez agregace a omezení (FUP)
- zapojení poskytovatele připojení v bezpečnostním projektu FENIX resp. veřejné adresy využívané školou jsou zapojeny do infrastruktury FENIX[5] nebo ISP splňuje alespoň technické standardy definované projektem FENIX – viz http://nix.cz/cs/file/NIX_PRAVIDLA_FENIX

2. Vnitřní konektivita školy (LAN)

Obecný popis: vnitřní síťové prostředí školy pořizované v rámci projektu může být řešeno pevnou sítí, bezdrátovou sítí, nebo kombinací těchto síťových technologií. Připojením je nutné pokrýt prostory dotčené

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

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

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

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

hlavním projektem, rovněž je možné pokrýt ostatní prostory školy, včetně chodeb, jídelen, internátu a dalších školských zařízení. Potřebnost a účelnost takového pokrytí musí být zdůvodněna ve studii proveditelnosti.

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

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

V oblasti pevné LAN musí projekt splňovat následující minimální parametry:

- Minimální konektivita stanic a dalších koncových zařízení zařízení 100Mbit/s fullduplex
- Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP,…)
- Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1Gbit/s fullduplex
- Páteřní rozvody mezi budovami v areálu realizovány prostřednictvím optických, metalických vláken popř. bezdrátovými spoji v licencovaném pásmu (povolení ČTÚ)
- Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3)[6] s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radiusbased MAC autentizace,…

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

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

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

- Minimálně pasivní zapojení[7] do federovaného systému eduroam (www.eduroam.cz). Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů.

3. Další bezpečnostní prvky

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

- Identity management systémy (IDM) – systém správy identit, řízení životního cyklu uživatelů, integrace do provozních a bezpečnostních systémů

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

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

- Centralizovaný autentizační systém napojení na systém správy identit (např. na bázi LDAP, AD, studijní a personální agendy apod.)
- Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty, blokace wifi v určitém čase)
- Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací a zpřístupnění jejich služeb)
- Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3954 nebo ekvivalent (NetFlow))
- Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie
- Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management)
- Systémy pro monitorování funkčnosti síťové a serverové infrastruktury (např. Nagios / Icinga)
- Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk)
- Nástroje pro centrální správu a audit ICT prostředků
- Systémy zálohování a obnovy dat serverové infrastruktury
- Systémy pro antivirovou ochranu zařízení, antispamovou ochranu poštovních serverů
- Zabezpečení přístupových protokolů (SSL/TLS) služeb (např. emailové služby, webové servery, studijní a ekonomické agendy) atp.
- Podpora vzdáleného přístupu (VPN)

EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

INTEGROVANÝ REGIONÁLNÍ OPERAČNÍ PROGRAM

SPECIFICKÁ PRAVIDLA PRO ŽADATELE A PŘÍJEMCE PRO INTEGROVANÉ PROJEKTY CLLD

SPECIFICKÝ CÍL 4.1

PRŮBĚŽNÁ VÝZVA Č. 68

PŘÍLOHA Č. 7B

STANDARD KONEKTIVITY STŘEDNÍCH ŠKOL A VYŠŠÍCH ODBORNÝCH ŠKOL

PLATNOST OD 3. 5. 2018

Tento dokument definuje základní technická kritéria cílového stavu školní síťové infrastruktury a přijatelnosti aktivit projektů naplňující strategický cíl IROP 2.4 v oblasti zajištění vnitřní konektivity škol a připojení k internetu - rozvoj vnitřní konektivity v prostorách škol a školských zařízení a připojení k internetu.

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

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

1. Konektivita školy k veřejnému internetu (WAN)

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

- šíře pásma (bandwidth) odpovídající 128kbps/student[1] nebo 512kbps/počítač[2] nebo taková šířka pásma, která neomezuje provoz zařízení a uživatelů[3]
- symetrické připojení bez agregace a omezení (FUP)
- vlastní nebo poskytovatelem přidělené veřejné IPv4 i IPv6 adresy
- plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack)
- validující DNSSEC resolver na straně školy
- podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení
- logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)
- síťové zařízení podporující rate limiting, antispoofing, ACL/xACL, rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality
- zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu, antivirovou kontrolou stahovaného obsahu
- možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků
- podpora DNSSEC a IPv6 protokolů pro služby školy dostupné online
- zapojení poskytovatele připojení v bezpečnostním projektu FENIX resp. veřejné adresy využívané školou jsou zapojeny do infrastruktury FENIX[4] nebo ISP splňuje

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

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

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

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

alespoň technické standardy definované projektem FENIX – viz http://nix.cz/cs/file/NIX_PRAVIDLA_FENIX

- u software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po celou dobu udržitelnosti projektu.

2. Vnitřní konektivita školy (LAN)

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

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

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

V oblasti pevné LAN musí projekt splňovat následující minimální parametry:

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

musí být součástí projektu prohlášení ISP, ze kterého bude patrné, že příslušné ASn propaguje do FENIX na základě smluvního vztahu některý ze členů FENIX.

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

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

- Podpora mechanismu izolace klientů
- Návrh topologie wifi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou ve v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů
- Centralizovaná architektura správy wifi sítě (centrální řadič, centrální management, tzv. thin access pointy, popř. alespoň centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravované access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení)
- Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD …)
- Podpora standardu IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz
- Minimálně pasivní zapojení[6] do federovaného systému eduroam (www.eduroam.cz). Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů.
- Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu

3. Další bezpečnostní prvky

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

- Identity management systémy (IDM) – systém správy identit, řízení životního cyklu uživatelů, integrace do provozních a bezpečnostních systémů
- Centralizovaný autentizační systém napojení na systém správy identit (např. na bázi LDAP, AD, studijní a personální agendy apod.)
- Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty, blokace wifi v určitém čase)
- Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací a zpřístupnění jejich služeb)
- Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3954 nebo ekvivalent (NetFlow))
- Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie
- Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management)
- Systémy pro monitorování funkčnosti síťové a serverové infrastruktury (např. Nagios/Icinga)
- Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk)

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

- Nástroje pro centrální správu a audit ICT prostředků
- Systémy zálohování a obnovy dat serverové infrastruktury
- Systémy pro antivirovou ochranu zařízení, antispamovou ochranu poštovních serverů
- Zabezpečení přístupových protokolů (SSL/TLS) služeb (např. emailové služby, webové servery, studijní a ekonomické agendy) atp.
- Podpora vzdáleného přístupu (VPN)