Příloha č. 1 kupní smlouvy - technické podmínky „Realizace WiFi připojení včetně bezpečnostního firewallu“

1. Předmět a účel přílohy smlouvy

Touto přílohou smlouvy jsou definovány technické podmínky předmětu kupní smlouvy, kterou se prodávající zavazuje k dodání a implementaci (zprovoznění) přístupových bodů k bezdrátové Wi-Fi síti a bezpečnostního firewallu (systému), včetně příslušných licencí.

2. Popis stávajícího a požadovaného stavu

2.1. Popis stávajícího stavu

Datová síť statutárního města Plzně je budována jako autonomní a vysoce dostupná IP síť s vlastními aktivními prvky, poskytující služby Statutárnímu městu Plzni, městským obvodům a městem zřízeným organizacím. Služby sítě jsou poskytovány jednotlivými logicky oddělenými IP sítěmi a zahrnují mimo jiné:

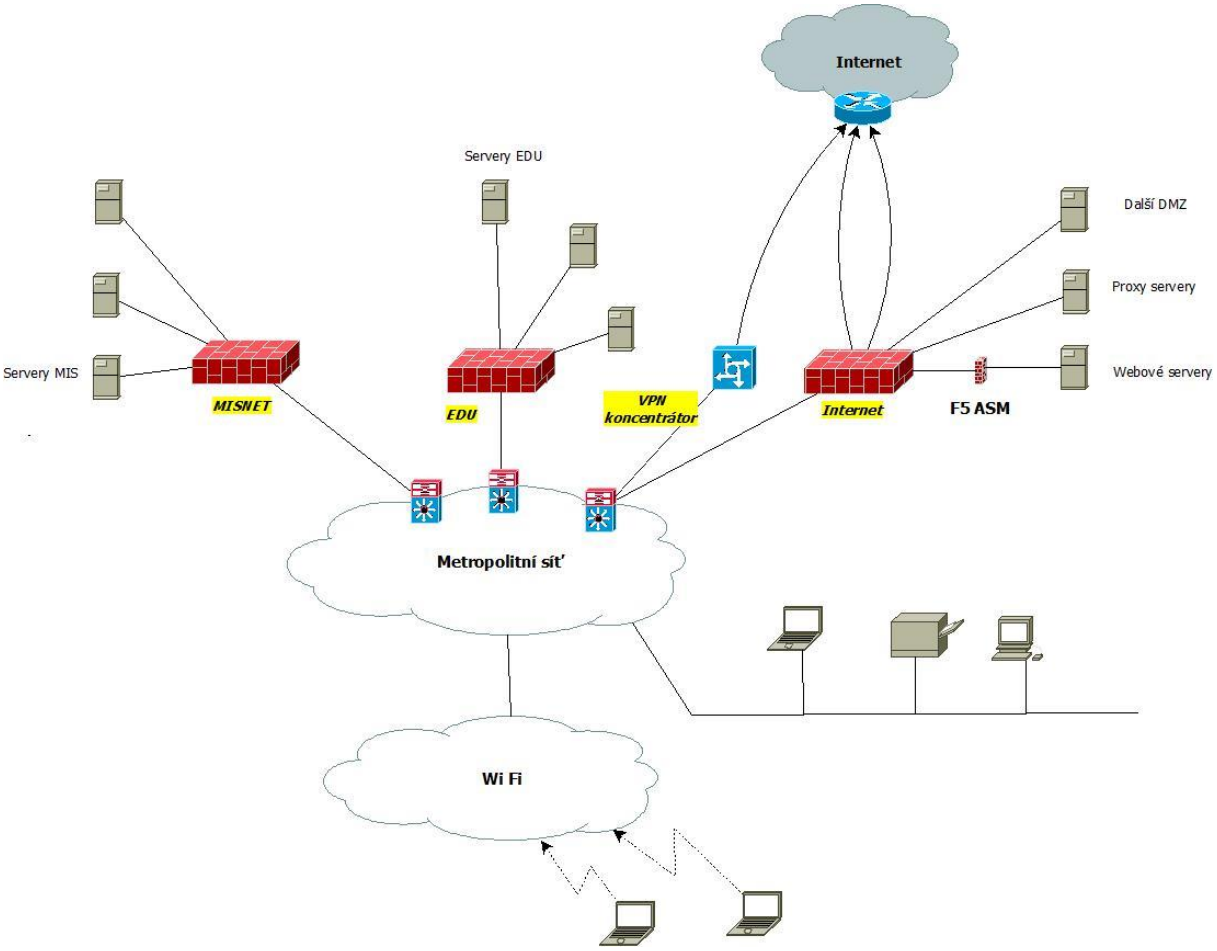
- informační systém „MIS“ – městský informační systém – poskytující podporu pro státní správu a samosprávu, řízení města a městských organizací (cca 1800 klientských PC a 2500 uživatelských identit)
- datová síť „EDU“ poskytující služby základním školám (cca 3000 klientských PC a 15000 uživatelských identit)
- Hlasové prostředí „JKP“ propojující hlasové systémy – pobočkové ústředny (50 ks) a IP telefony, celkem 4000 poboček
- Datová síť „MKS“ – městský kamerový systém – zahrnující přenosové prostředí pro více než sto kamer, 6 sledovacích pracovišť různé velikosti a datová úložiště
- Datová síť „PUBLIC“ poskytující WiFi hotspoty ve veřejně dostupných prostorech (např. pobočky Knihovny města Plzně, apod.)

Celé toto prostředí je propojeno více než 120 km optických přenosových tras a zahrnuje více než 400 aktivních prvků, 6 vysokokapacitních bezdrátových spojů, stovky bezdrátových přístupových bodů.
Hlavní informační a fyzická aktiva datové sítě statutárního města Plzně představuje více než 200 serverů (aplikačních, souborových a databázových) a sdílená datová úložiště. Tato aktiva jsou soustředěna ve dvou geograficky oddělených datových centrech propojených nezávislými optickými trasami. Datová centra jsou schopna vzájemné zálohy u kritických systémů.

Klíčovým bezpečnostním systémem datové sítě statutárního města Plzně je cluster dvou vysoce propustných firewallů, nad kterými jsou nakonfigurovány tři virtuální firewally (kontexty). Každý z virtuálních kontextů připojuje k datové síti logicky ucelené skupiny serverů, které poskytují uživatelům odpovídající sady služeb. Servery jsou síťově rozděleny do více než 20 zón a jsou od klientů a od sebe navzájem odděleny virtuálními firewally.
Aktuálně v síti statutárního města Plzně funguje active – active cluster složený ze dvou jednotek Cisco ASA.. Stávající řešení neobsahuje pokročilé techniky detekce škodlivého SW a nežádoucí komunikace.

Na následujícím obrázku je zjednodušeně znázorněna současná topologie datové sítě:
kontext „MISNET“ připojující k metropolitní síti servery MIS (celkem 5 segmentů)
kontext „EDU“ připojující k metropolitní síti servery EDU, systémy Plzeňské karty a Plzeňské vstupenky (celkem 4 LAN segmenty)

kontext „Internet“, který řídí připojení klientských systémů metropolitní sítě k Internetu a zprostředkovává uživatelům na Internetu přístup k elektronickým službám datové sítě statutárního města Plzně. Celkem jsou servery umístěny ve 12 různých demilitarizovaných zónách (DMZ). Kritické Web servery jsou soustředěné do jedné z DMZ a dále chráněné pomocí Web Apllication Firewallu (F5 ASM).
Dalším důležitým bezpečnostním systémem je VPN koncentrátor sloužící pro připojení jednotlivých uživatelů přes Internet (Remote Access VPN) a připojující lokality mimo dosah městské sítě (Site to Site VPN), typicky mateřské školy.



Aktuálně v síti statutárního města Plzně funguje centralizované wifi řešení postavené na bezdrátových kontrolérech Cisco Wireless LAN Controller 5520 s využitím „odlehčených“ přístupových bodů Cisco, tzv. lightweight access point.

2.2. Popis požadovaného stavu

Cílovým stavem je zvýšit úroveň ochrany informačních, aplikačních a fyzických aktiv datové sítě statutárního města Plzně rozšířením již implementovaných bezpečnostních systémů o WiFi připojení včetně bezpečnostního firewallu.

Předpokládané nasazení nového bezpečnostního firewallu je takové, že dojde k rozšíření síťové infrastruktury o active – active cluster složený ze dvou fyzických jednotek firewallů. V clusteru budou

konfigurovány virtuální instance firewallů. Jedna z instancí bude sloužit pro připojení prostředí EDU sítí k internetu a bude používat pokročilé techniky k detekci síťových útoků, nežádoucí komunikace, škodlivého software a další. Ostatní virtuální instance budou řídit provoz k interním serverům EDU, MISNET a další.

Předpokládané nasazení 16ks WiFi přístupových bodů je takové, že dojde k rozšíření stávajícího, již provozovaného, centralizovaného wifi řešení o 16ks přístupových bodů včetně licencí. WiFi přístupové body budou zapojeny do stávajících přístupových switchů a spravovány pomocí stávajících bezdrátových kontrolérů.

3. Rozsah předmětu plnění

- dodávka WiFi připojení včetně bezpečnostního firewallu (16ks WiFi přístupových bodů a 2ks bezpečnostního hardwarového zařízení firewallu), viz. bod 3.1
- zprovoznění WiFi připojení včetně bezpečnostního firewallu, viz. bod 3.2
- testovací provoz, viz. bod 3.3.
- akceptace díla, viz. bod 3.4

3.1. Dodávka systému, funkční a technická specifikace WiFi připojení včetně bezpečnostního firewallu

Předmětem dodávky jsou:

a) 16ks shodného hardwarového zařízení „WiFi přístupový bod“, tabulka a)
b) 2ks shodného hardwarového zařízení „bezpečnostní firewall“ , tabulka b)

Pozn. Každé zařízení z požadovaného počtu kusů musí samostatně splnit požadované parametry uvedené v tabulce a) a v tabulce b). Požadované parametry uvedené v tabulkách jsou minimální a musí být ve všech případech dodrženy nebo vylepšeny.

Tabulka a) Požadovaná funkční a technická specifikace WiFi přístupového bodu

Požadavek č.	Požadovaná funkční a technická specifikace WiFi přístupového bodu
1.	kompatibilita se stávajícím centralizovaným řešením
2.	licence přístupového bodu pro stávající centralizované řešení
3.	požadavky na vstupní napájení: podpora 802.3at PoE+ a 802.3at power injector
4.	integrované antény 2,4 i 5 GHz
5.	4x4 MIMO, 3x spatial stream
6.	podpora a provoz ve standardu 802.11n - šířka kanálu 20, 40 MHz
7.	podpora a provoz ve standardu 802.11ac Wave 2 - šířka kanálu 20, 40, 80, 160 MHz
8.	802.11 dynamic frequency selection (DFS)
9.	Wi-Fi Alliance certifikace a, b, g, n, ac
10.	Min. 2 Ethernet porty ◦ 100/1000BASE-T (RJ-45) ◦ kategorie kabeláže min. CAT 5e ◦ management console port (RJ-45)

Tabulka b) Požadovaná funkční a technická specifikace bezpečnostního firewallu

Požadavek č.	Požadovaná funkční a technická specifikace bezpečnostního firewallu
1.	Dodávaná firewall platforma je ve formě samostatného hardware zařízení (fyzický FW, appliance)
2.	Dodávaná firewall platforma musí být uvedena v Gartner Magic Quadrant pro Enterprise Network Firewalls za roky 2015-2017 minimálně 2x v kvadrantu Leaders nebo Challangers
3.	Instalace do standardního 19" RACKu (Rack mount kit v ceně zařízení)
4.	Lokální HDD, min 2x800GB RAID1, pro případ výpadku centrálního management log serveru
5.	Hot-swappable redundantní napájecí zdroje (AC)
6.	Hot-swappable redundantní ventilátory
7.	Vysoce dostupné řešení bezpečnostního firewallu s možností režimu active-standby a active-active
8.	Vyhrazené fyzické síťové rozhranní pro dohled a konfiguraci
9.	Počet požadovaných fyzických síťových rozhraní, minimálně 10x 10/100/1000baseT, podpora agregace fyzických interface stejného typu dle IEEE 802.3ad (bond rozhranní)
10.	Počet požadovaných fyzických síťových rozhraní, minimálně 10x 10Gb SFP+ rozhraní, podpora agregace fyzických interface stejného typu dle IEEE 802.3ad (bond rozhranní)
11.	Možnost rozšíření: minimálně 4x 40Gb QSFP+ rozhraní
12.	Součástí dodávky bude pro každý fyzický FW 3 ks (celkem pro obě zařízení tedy 6 ks) 10GBASE-LR SFP+. Je-li použití síťových portů licencováno, musí být licence na všechny porty součástí dodávky.
13.	Propustnost Firewallu, minimálně 75 Gbps (RFC 3511, 2544, 2647, 1242)
14.	Propustnost IPS, minimálně 20 Gbps (se všemi zapnutými filtry)
15.	Propustnost VPN, minimálně 14 Gbps
16.	Propustnost NGFW (Firewall, IPS, Aplikační kontrola), minimálně 20 Gbps
17.	Propustnost Threat ochrany (Firewall, IPS, Anti-Bot Aplikační kontrola, Antivir, URL filtering,), minimálně 17 Gbps
18.	Počet nových spojení za vteřinu (CPS) minimálně 200.000
19.	Počet současných spojení, minimálně 6.000.000
20.	Podpora VPN pro vzdálený přístup (IPSec, SSL), minimálně 150 současně navázaných VPN spojení / klientů, licence (je-li potřeba) pro požadovaný počet musí byt součástí nabídky
21.	Podpora Site-to-Site VPN (IPSec), minimálně 50 současně navázaných VPN tunelů, licence (je-li potřeba) pro požadovaný počet musí byt součástí nabídky
22.	Požadované funkcionality včetně potřebných licencí: firewall, ips, kontrola aplikací, url filtering, antivirus, botnet blokace, rozpoznávání uživatelských identit
23.	Podpora Dual stack konfigurace IPv4/IPv6 a to včetně konfigurace bond rozhraní a sub-rozhraní v bondu
24.	Okamžitě použitelné předdefinované IPS politiky

25.	Možnost definice IPS výjmek dle kombinace: src IP + dst IP + service + útok/signatura
26.	Řízení politky na základě uživatelských skupin z Active Directory
27.	Podpora transparentní Kerberos autentikace pro Single Sign On
28.	Podpora software agenta na koncové stanice pro přesné získavaní identit, bez nutnosti instalace na Windows Server, min. pro systémy Windows, s podporou ipv6, případná licence pro 5000 agentů musí být součástí nabídky
29.	Detekce a řízení síťových aplikací. Minimální počet rozpoznávaných aplikací 6000
30.	Možnost příchozí a odchozí HTTPS inspekce pro konkrétní virtuální firewall instanci
31.	Ochrana proti známému malwaru
32.	Funkce Blokovaní botnet komunikace na základě reputace, signatur a behaviorální analýzy
33.	Detekce a prevence DNS tunnelingu
34.	Podpora debuggování problémových scénářů na úrovni L2 - L7.
35.	Každý fyzický FW musí umožnovat vytváření a provozování virtuálních FW instancí Počet dodávaných licencí pro virtuální firewall instance minimálně 10 ks pro každý fyzický FW
36.	Počet dodávaných licencí pro dedikované virtuální prvky zabezpečující přepínaní a směrovaní (L2, L3), jsou-li potřeba nad rámec licencí pro virtuální firewall instance, minimálně 10 ks pro každý fyzický FW
37.	Load balancing virtuálních firewall instancí mezi fyzické členy active – active clusteru firewall platformy s možností kontrolovat, na kterém členu clusteru je konkrétní virtuální FW instance aktivní
38.	Podporované režimy virtuálních firewall instancí: L3 routovací a L2 transparentní režim v četně možnosti provozovat oba režimy (v různých instancích)
39.	Vytváření dedikovaných virtuálních instancí zabezpečujících přepínaní a směrovaní paketů mezi virtuálními firewally a mezi virtuálními firewally a externími segmenty.
40.	Každá virtuální firewall instance musí implementovat: vlastní bezpečnostní politiku, stavové, routovací a ARP tabulky, síťové nebo virtuální rozhraní.
41.	Řízení hardware zdrojů pro jednotlivé virtuální firewall instance (CPU, paměť).
42.	Dynamické řízení hardware zdrojů pomocí nastavení priorit pro jednotlivé virtuální firewall instance.
43.	Monitoring využívaných zdrojů pro jednotlivé virtuální firewall instance (počet spojení, využívaní CPU, paměť)
44.	Možnost vypnutí IPS ochrany pro konkrétní virtuální firewall instance v případě přetížení hardware zdrojů (využití CPU nebo fyzické paměti) nad definovanou prahovou hodnotu.
45.	Přímá propagace veřejných IP adres virtuálních firewall instancí ze stejného síťového rozsahu, bez nutnosti NAT-ovaní (virtuální L2 propoj v rámci virtualizační platformy).
46.	Kontrola síťových protokolů na aplikační vrstvě, včetně dynamického otevíraní portů pro specifický síťové protokoly (DCE-RPC, FTP, SIP, H.323, MGCP) i pro konkrétní virtuální firewall instanci.
47.	Kontrola síťových protokolů na aplikační vrstvě v případě využívaní nestandardních portů i pro konkrétní virtuální firewall instanci.

48.	Řízení přístupu MS DCE-RPC na základě UUID i pro konkrétní virtuální firewall instanci.
49.	Geolokace a kontrola síťových protokolů dle zeměpisné polohy pro konkrétní virtuální firewall instanci
50.	Aktualizace bezpečnostích signatur a geolokačních dat min. 2x týdně
51.	Management musí být fyzicky oddělený od firewall platformy – jako samostatný HW nebo jako SW appliance určená pro provoz ve virtuálním serveru. V případě, že je nutná licence pro management, musí být součástí nabídky.
52.	Konsolidovaný centrální management: správa politik a analýza logů na jedné platformě
53.	Centrální management musí umožnit připojení minimálně 10 současných uživatelů. Je-li tato funkcionalita licencována, musí být licence součástí dodávky.
54.	Centrální management systému musí umožňovat autentizaci administrátorů alespoň pomocí Microsoft Active Directory nebo RADIUS serveru.
55.	Funkcionalita ukládaní, filtrování a korelace logů, analýzy a správy bezpečnostních událostí s předefinovanými pohledy/dotazy
56.	Možnost vytváření uživatelsky definovatelných reportů a přehledů a jejich automatické zasílání emailem ve formátu PDF
57.	Možnost propojení se systémem SIEM třetí strany
58.	Automatická verifikace politiky (např. proti redundanci, překryvu a inkonzistenci pravidel)
59.	Podpora vyhledávaní v pravidlech, vyhledávaní textových výrazů/objektů/IP adres nebo prohledávaní všech objektů.
60.	Podpora administrátorských profilů s možností přidělování práv (read only, red-write, none) pro jednotlivé skupiny administračních funkcí
61.	Definice oddělených politik s možností práce více administrátorů najednou (každý na přidělené politice)
62.	Možnost přidělení práv administrátorům jen pro definovanou politiku/virtuální instanci firewallu
63.	Hit count statistiky pro jednotlivá pravidla za účelem optimalizace bezpečnostní politiky
64.	Fulltextové prohledávaní logů, včetně technologie indexace pro účinné a rychlé prohledávání logů/záznamů v řádu milionů
65.	Integrovaný monitoring musí poskytovat grafické rozhraní pro sledování parametrů v reálnem čase (využití paměti, CPU, počet navázaných spojení, počet nově otevřených spojení za sekundu, propustnost, atd …).
66.	Interní certifikační autorita za účelem vydávaní a správy PKI certifikatů pro jednotlivé firewall a VPN (může být zabezpečeno produktem třetí strany, musí být součástí nabídky)
67.	Management log server musí zpracovat min. 20000 logů/s
68.	Požadujeme historii uložených stavových informací (logů a eventů) min. 12 měsíců. Minimální podporovaná velikost diskové kapacity pro dlouhodobé ukládaní log záznamů a eventů na management serveru (je-li disková kapacita omezena licencí, licence pro požadovanou velikost musí byt součástí nabídky), min. 16 TB

69.	Požadována licence pro centrální správu a dedikovaný reporting, minimálně pro výše požadovaný počet virtuálních firewall instancí
70.	Podpora revizí bezpečnostních politik, jejich verzování.
71.	Podpora auditních informací u změn bezpečnostní politiky.

3.2. Zprovoznění WiFi připojení včetně bezpečnostního firewallu

Zprovozněním WiFi připojení včetně bezpečnostního firewallu se rozumí:

- Zapojení a instalace jednotlivých komponent (jedná se o 2ks bezpečnostního firewallu, WiFi AP si nainstaluje a zapojí kupující vlastními silami)
- Základní konfigurace zařízení (jedná se o 2ks bezpečnostního firewallu, WiFi AP si nainstaluje a zapojí kupující vlastními silami)
- Rozšířená konfigurace systému (jedná se o 2ks bezpečnostního firewallu, WiFi AP si nainstaluje a zapojí kupující vlastními silami)
- Provedení komplexních testů dle testovacích scénářů

Zhotovitel po úspěšném zprovoznění WiFi připojení včetně bezpečnostního firewallu dodá objednateli jako součást předmětu plnění podrobnou dokumentaci dodávaného systému, včetně kompletního popisu, nastavení a konfigurace daného řešení tak, aby jej bylo možné nadále provozovat a udržovat.

Objednatel požaduje dodání dokumentace v následující logické struktuře:

- provozní dokumentace v českém jazyce
- administrátorská příručka
- testovací scénáře funkčnosti bezpečnostního firewallu v českém jazyce
- plány obnovy bezpečnostního firewallu v českém jazyce

Popis plánů obnovy bude zpracován v míře podrobnosti použitelné pro zařazení do celkového plánu obnovy (Disaster Recovery Plan).
Součástí této dokumentace musí být popis instalace a konfigurace bezpečnostního firewallu v takovém rozsahu a detailu, který umožní znovu zprovoznit celý systém v nově nainstalovaném čistém prostředí bez pomoci zhotovitele.

Dokumentace bude dodána ve formátu MS Office 2013 a vyšší tak, aby umožňovala následnou editaci objednatelem.

Míra detailu dokumentace bude taková, aby objednatel byl s jejich pomocí sám schopen proškolit další osoby.

Dokumentace musí kromě obecné práce se systémem obsahovat i specifické informace o konkrétní implementaci a konfiguraci řešení nasazené u objednatele.

Veškerá dokumentace musí splňovat požadavky na vizuální identitu Integrovaného operačního programu.

3.3. Testovací provoz (právo objednatele na testování dodaného a zprovozněného WiFi připojení včetně bezpečnostního firewallu před celkovou akceptací dodaného díla)

3.3.1. Povinnosti objednatele v průběhu testovacího provozu:

Testovací provoz je zahájen objednatelem na základě celkového zprovoznění WiFi připojení včetně bezpečnostního firewallu.
Délka testovacího provozu objednatelem je stanovena na 7 kalendářních dnů
Testovací provoz slouží k ověření bezchybného chodu systému v reálném provozu.
Testovací provoz obsahuje provedení komplexních testů dle testovacích scénářů objednatelem za přítomnosti a spolupráce zhotovitele

- Provedení bezpečnostních testů WiFi připojení včetně bezpečnostního firewallu objednatelem za přítomnosti a spolupráce zhotovitele
- Provedení zátěžových testů WiFi připojení včetně bezpečnostního firewallu objednatelem za přítomnosti a spolupráce zhotovitele
- Provedení komplexních testů dle testovacích scénářů objednatelem za přítomnosti a spolupráce zhotovitele

Objednatel a zhotovitel o průběhu testování vyhotoví testovací protokol.

3.3.2. Povinnosti zhotovitele v průběhu testovacího provozu:

- Ode dne ukončení testování objednatelem je zhotovitel povinen nejpozději do 5 kalendářních dnů odstranit veškeré závady zjištěné v průběhu testování a uvedené v testovacím protokolu.

3.4. Akceptace díla

Zhotovitel je povinen nejdéle do 72 kalendářních dnů od účinnosti této smlouvy dodat a zprovoznit předmět této smlouvy, včetně odstranění všech chyb identifikovaných v průběhu testovacího provozu.

4. Harmonogram plnění (řešení)

Harmonogram zprovoznění WiFi připojení včetně bezpečnostního firewallu v prostředí SPRÁVY INFORMAČNÍCH TECHNOLOGIÍ MĚSTA PLZNĚ, příspěvkové organizace:

Tabulka termínů plnění

	Termín :	Popis činnosti
1.	Do 60 dnů ode dne účinnosti této smlouvy	Celkové dodání a zprovoznění WiFi připojení včetně bezpečnostního firewallu viz. bod 3.1 a 3.2 této přílohy, Včetně dodání dokumentace v následující logické struktuře: • provozní dokumentace v českém jazyce • administrátorská příručka • testovací scénáře funkčnosti systému v českém jazyce • plány obnovy v českém jazyce (první předávací protokol)
2.	Do 67 dnů ode dne účinnosti této smlouvy	Testovací provoz dle bodu 3.3.1. této přílohy (druhý předávací protokol – testovací protokol)
3.	Do 72 dnů ode dne účinnosti této smlouvy	Celková akceptace díla dle bodu 3.4. této přílohy (po odstranění vad dle bodu 3.3.2. této přílohy (třetí předávací protokol – akceptace díla)

Dohoda smluvních stran k termínům plnění:
Smluvní strany se podpisem této smlouvy dohody, že pokud poslední kalendářní den kteréhokoliv ze shora uvedených termínů je dnem pracovního klidu, přesouvá se poslední den takového termínu na první pracovní den následující po ukončení takového termínu.