

VÝČET ŘÍDÍCÍCH DOKUMENTŮ PPSP A POPIS JEJICH OBSAHU

V této příloze je uvedena specifikace dokumentů PPSP. Dokumenty budou dokončeny v etapě implementace PPSP a v okamžiku jejich akceptace zmocněnci pro jednání ve věcech odborných a technických za obě smluvní strany se stanou Řídícími dokumenty pro etapu implementace i provozu PPSP.

Aktualizace Řídících dokumentů projektu bude součástí změnových řízení v provozní fázi Projektu PPSP.

1. Technický projekt

Vytvoření dokumentu Technický projekt je součástí činností realizovaných v implementační etapě Projektu PPSP v souladu s tabulkou závazných milníků projektu, uvedenou v odstavci 5.3 Smlouvy.

Dokument obsahuje následující oblasti:

- Návrh celkové infrastrukturní architektury
- Návrh adresního plánu
- Návrh architektury sítě
- Návrh architektury LPARů
- Návrh rozmístění HW v DC a požadavky na stěhovací trasy, napájení, klimatizaci a protipožární zabezpečení
- Návrh architektury SAN a rozdělení do SAN zón
- Návrh architektury diskových prostor
- Návrh architektury clusterů
- Návrh architektury monitoringu
- Návrh architektury a procesů zálohování
- Požadavky na konfigurace HSM modulů (kryptokaret)
- Návrh akceptačních testů
- Přesná specifikace součinností implementátora aplikací IISSP s ohledem na implementaci clusteringu a zálohování
- Součinnost objednatele

Prováděcí projekt bude základním implementačním dokumentem, podle kterého bude prováděna vlastní instalace a implementace infrastruktury PPSP. Na jeho vytváření se budou podílet pracovníci všech zúčastněných stran včetně implementátora informačního systému IISSP.

Prováděcí projekt bude po vypracování předložen k akceptaci objednateli.

1.1 Požadovaná součinnost

Pro zahájení prací na technickém projektu dodá objednatel dokumenty obsahující tyto položky:

- 1.1.1 Návrh adresního plánu sítě podle požadavků aplikací IISSP
- 1.1.2 Návrh jmenných konvencí pro hostname v aplikačních sítích
- 1.1.3 Všechny požadavky aplikací IISSP na nastavení operačních systémů, zejména
 - Přesnou verzi operačního systému včetně oprav (Technology Level a Service Pack)

- Požadované nainstalované SW balíčky operačního systému
 - Požadované konfigurační parametry jádra operačního systému a TCP/IP subsystému
 - Další potřebná nastavení operačního systému
 - Požadované konfigurace HSM modulů (kryptokaret)
- 1.1.4 Výkonové požadavky na jednotlivé subsystémy aplikací IISSP**
- Požadovaný počet SAPS pro fáze 80% a 100% výkonu infrastruktury PPSP
 - Požadované velikosti paměti pro fáze 80% a 100% výkonu infrastruktury PPSP (musí reflektovat celkovou dostupnou paměť navržených systémů, příloha 3 kapitola 2.1 Dodávka serverů)
 - Požadované parametry budou uvedeny pro jednotlivé LPARy a jednotlivá prostředí (produkční, testovací, školící a vývojové)
- 1.1.5 Požadavky na diskové prostory jednotlivých aplikací IISSP a to formou tabulky obsahující**
- Požadované diskové kapacity pro jednotlivé subsystémy aplikací IISSP (LPARy)
 - Rozdělení požadovaných kapacit do filesystémů a názvy těchto filesystémů (mount pointy)
 - Růst kapacit jednotlivých filesystémů během 5 let provozu PPSP
 - Hodnoty změn dat v jednotlivých filesystémech za jednotku času a to zejména KB/sec ve špičce (pro nastavení synchronního mirroringu mezi diskovými poli) a souhrny za den, týden a měsíc (pro specifikaci zálohovacích postupů).
 - Specifické požadavky na parametry filesystémů, pokud jsou.
 - Požadované parametry budou uvedeny pro jednotlivé LPARy a jednotlivá prostředí (produkční, testovací, školící a vývojové)
- 1.1.6 Přesné verze aplikačního SW (SAP, Oracle).**
- 1.1.7 Požadavky na aplikační komunikaci informačního systému IISSP**
- Celkové komunikační schéma informačního systému IISSP
 - Komunikační toky jednotlivých subsystémů (LPARů) – požadavky na jednotlivá propojení, specifikace portů, datových toků a požadavky na nastavení Firewall/ACL
 - Požadované parametry budou uvedeny pro jednotlivé LPARy a jednotlivá prostředí (produkční, testovací, školící a vývojové)
- 1.1.8 Konektivity do vnějších sítí LAN MF, WAN GOVBONE, internet**
- 1.1.9 Nákrasy jednotlivých sálů pro primární a sekundární datové centrum, obsahující rozmístění komunikačních racků (připojení do vnějších sítí a propojení mezi datovými centry) a napájecích přívodů.**

Výše uvedené dokumenty budou sloužit jako vstupní údaje pro proces vytváření dokumentu Technického projektu a objednatel je poskytne dodavateli nejpozději k začátku etapy Technický projekt, viz Harmonogram projektu.

Objednatel se bude podílet na procesu vytváření dokumentu Technický projekt a poskytne v potřebném rozsahu specialisty na jednotlivé části dodávky, zejména síťového specialistu a specialistu na bezpečnostní otázky. Součástí projektového týmu budou i pracovníci implementátora aplikací IISSP za všechny oblasti požadavků těchto aplikací (zejména datové prostory a kapacity, zálohování, instalace na OS AIX, aplikační komunikace). Implementátor IISSP bude zodpovědný za návrh klientské části zálohování, tzn. procedury a skripty na úrovni aplikací IISSP (SAP a databáze) a požadavky na provádění záloh (co a jak často, dobu úschovy a expiraci).

2. Bezpečnostní projekt

Vytvoření dokumentu Bezpečnostní projekt je součástí činností realizovaných v implementační etapě Projektu PPSP v souladu s tabulkou závazných milníků projektu, uvedenou v odstavci 5.3 Smlouvy. Rozsah dokumentu Bezpečnostní projekt vychází z následujících dokumentů závazných pro STC a Dodavatele v této oblasti zejména:

- ČSN ISO/IEC 20000-1,2,
- ČSN ISO/IEC 27001,
- Bezpečnostní politika ICT MF ČR,
- Interní směrnice SRBI STC.

Pro PPSP bude vypracován Bezpečnostní projekt infrastruktury (tj. sada bezpečnostních dokumentů) v souladu se normou ČSN ISO/IEC 27001. Obsah bezpečnostní dokumentace bude vymezen šíří poskytované služby:

- Komunikační infrastruktury v rámci primárního a sekundárního datového centra. Hranicí komunikační infrastruktury je připojení na firewally, poskytované a provozované zadavatelem.
- Hardware serverů a zálohovacích systémů v rámci primárního a sekundárního datového centra. Zabezpečení provozu aplikací, včetně logických přístupů je zajištěno zadavatelem.
- Monitoringu hardware systémů v rámci primárního a sekundárního datového centra.

2.1 Bezpečnostní projekt infrastruktury PPSP bude sestávat ze samostatných dokumentů:

2.1.1 Administrátorské a uživatelské bezpečnostní příručky infrastruktury PPSP

- Systémová bezpečnostní příručka infrastruktury PPSP
- Bezpečnostní provozní směrnice pro administrátory infrastruktury PPSP
- Bezpečnostní provozní směrnice pro bezpečnostního správce PPSP:
 - Bezpečnostní provozní směrnice pro správu PPSP
 - Bezpečnostní provozní směrnice pro zvládání bezpečnostních incidentů

2.1.2 Havarijní plány a plány obnovy infrastruktury PPSP

Vypracování havarijních plánů infrastruktury PPSP bude probíhat v několika na sebe navazujících etapách:

2.1.2.1 Analýza dopadů havárie – BIA

Business Impact Analysis (dále BIA) je klíčovým krokem v procesu havarijního plánování. Umožňuje charakterizovat systémové požadavky, procesy a vzájemné závislosti tak, aby bylo možno determinovat požadavky a priority havarijního plánování.

2.1.2.2 Politika havarijního plánování

Havarijní plány musí být vytvořeny na základě jasně definované politiky. Ta definuje celkové cíle, organizační rámec a zodpovědnosti pro havarijní plánování ICT. Cílem této etapy je vytvoření základní politiky havarijního plánování. Politika havarijního plánování definuje na úrovni managementu strategická východiska a principy havarijního plánování v prostředí zákazníka.

2.1.2.3 Strategie obnovy klíčových částí infrastruktury IISPP a plány obnovy

Cílem této etapy je specifikovat sadu parametrů, informací a dalších zdrojů, které jsou nutné pro zajištění procesu obnovy infrastruktury PPSP (navrácení do původního stavu). Specifikace musí zohledňovat úroveň hrozeb působících na kritickou část infrastruktury PPSP (na základě výsledků vyplývajících z Business Impact Analysis).

Fáze obnovy – návrh opatření a postupů směřujících k obnově prozatímní funkčnosti poškozených částí infrastruktury PPSP v závislosti na zvolené strategii obnovy (sekvence obnovovacích aktivit). Cílem bude zajistit funkčnost systému v rozsahu stanoveným havarijním plánem. Obnovovací procedury budou vypracovány v sekvenčním formátu a budou zpracovány pro jednotlivé komponenty strategických IS.

2.1.2.4 Požadovaná součinnost

Objednatel dodá dokumenty:

- Bezpečnostní politika ICT MF ČR,
- Interní směrnice SŘBI STC,
- Analýza rizik Projektu IISSP,
- Případně jiné relevantní dokumenty, jejichž požadavky mají být zahrnuty do bezpečnostního projektu.

Objednatel poskytne součinnost odpovědných pracovníků pro oblast bezpečnosti pro stanovení technických a bezpečnostních požadavků na provozování PPSP v termínech vypracovávání bezpečnostního projektu.

3. Plán realizace a podpory provozu PPSP

Vytvoření dokumentu provozního manuálu je součástí činností realizovaných v přípravné a implementační etapě. Plán realizace a podpory provozu PPSP bude obsahovat následující informace:

- rozpracování podpory provozu jednotlivých komponent PPSP v etapě provozu – provozní manuál
- ostatní náležitosti a součinnost související s plánem realizace.

Struktura provozního manuálu bude obsahovat kapitoly podle tabulky níže:

Struktura provozního manuálu
Definice pojmů a zkratk Řízení služeb (Help Desk služba, On –site zásahy, vzdálené zásahy) Priority provozu
Popis provozních procesů Komunikační plán Řízení změn Řízení problémů Řízení bezpečnosti Řízení kontinuity Řízení kvality
Definice technického rozhraní Rozsah spravované infrastruktury
Definice SLA a reportování Akceptace provedených služeb Podklady pro fakturaci – vzor akceptačního protokolu
Bezpečnost provozu v podobě citace na relevantní část bezpečnostního projektu

Struktura provozního manuálu
Havarijní plán a plán obnovy v podobě citace na relevantní část bezpečnostního projektu
Organizační struktura Kontakty Oblasti odpovědnosti

3.1 Požadovaná součinnost

Objednatel bude spolupracovat na vytváření dokumentu a předá všechny nezbytné podklady týkající se provozu datových center, zejména požadovaná organizační a bezpečnostní pravidla, vzory akceptačních a report dokumentů.

4. Průběžná aktualizace dokumentů

Dokumenty budou aktualizovány a doplňovány v rámci podpory provozu a správy infrastruktury. Budou pravidelně (minimálně 1x měsíčně) revidovány a aktualizovány při každé relevantní změně související dokumentace nebo v dodané infrastruktuře. Všechny provedené změny dokumentu budou akceptované Objednatelem a verzované.

5. Rozpis cen

Rozpis cen je uveden v příloze č.11 Smlouvy.