**PŘÍLOHA Č. 6 – SPECIFIKACE IT PROSTŘEDÍ**

**OBSAH**

[1 Technologie 2](#_Toc536361718)

[1.1 Databáze 2](#_Toc536361719)

[1.2 Operační systémy 2](#_Toc536361720)

[1.3 Virtualizace 2](#_Toc536361721)

[2 Vzdálená správa 2](#_Toc536361722)

[2.1 Management systému 2](#_Toc536361723)

[2.2 Podpora uživatelů 2](#_Toc536361724)

[2.3 VPN tunely 2](#_Toc536361725)

[3 Specifikace IT infrastruktury 2](#_Toc536361726)

[3.1 Servery a disková pole 2](#_Toc536361727)

[3.2 Síťová topologie 3](#_Toc536361728)

[3.3 Segmentace sítě 3](#_Toc536361729)

[3.4 Load balancery 4](#_Toc536361730)

[3.5 Zálohování 4](#_Toc536361731)

[3.6 Plány obnovy 4](#_Toc536361732)

[3.7 Provozní monitoring 4](#_Toc536361733)

# VZDÁLENÁ SPRÁVA

## Management systému

Pro přístup do sítě Objednatele bude v dedikované síťové zóně vytvořen terminálový server, který bude sloužit pro Poskytovatele jako vstupní bod do sítě justice a z něj bude primárně provádět činnosti, které jsou pro plnění Servisní smlouvy nezbytné.

Pro připojení na tento terminálový server je využívána technologie Microsoft TSG. Ověřování probíhá pomocí čipové karty, kterou dostanou pověření zaměstnanci Zhotovitele na základě předloženého vyplněného a podepsaného standardizovaného formuláře.

## Podpora uživatelů

Pro podporu uživatelů Objednatele lze využít technologie Adobe Connect, kterou disponuje Objednatel. Sdílení obrazovky lze nastavit pouze směrem od uživatele směrem k Poskytovateli.

## VPN tunely

Pro potřeby plnění Servisní smlouvy nebudou vytvářeny IPSEC VPN tunely.

## Síťová topologie

Přehledová síťová topologie je znázorněna na tomto schématu

Servery disponují síťovými kartami o kapacitě 10Gbit/s. Servery mezi sebou mají 20Gbit/s propoj a servery napříč lokalitami mají taktéž propojení o rychlosti 80Gbit/s.

* Internetová linka má nyní kapacitu 2Gbit/s.
* Linka do sítě KIVS (Komunikační infrastruktura veřejné správy) má nyní kapacitu 10Gbit/s.

## Segmentace sítě

Objednatel předpokládá pro implementaci Systému vytvoření minimálně jednoho dedikovaného síťového rozsahu pro vnitřní komponenty Systému o velikosti 0/24 , který bude mít defaultní gateway na centrální firewallu. Veškerá komunikace se síťovými zařízeními systému bude tedy kontrolována firewallem. Základní nastavení firewallu Objednatele je v režimu „all block“ tzn. veškerá komunikace je blokována a pouze se povolují nezbytné komunikace.

## Zálohování

Zálohování všech komponent Systému bude realizováno prostřednictvím zálohovacího řešení Objednatele.

## Plány obnovy

Poskytovatel v rámci provedení Systému vždy vytvoří dokumentaci jednoznačně upravující kroky vedoucí k zajištění plné obnovy služeb Systému po havárii mající globální dopad na chod Systému s ohledem na minimalizaci dopadů. Dokumentace DRP (*Disaster Recovery Plan*) musí být zpracována do nejmenšího detailu, to znamená vytvoření detailního postupu obnovy každé komponenty včetně popisu všech kroků vedoucí k její obnově. Plány obnovy musí být také v souladu s metodikou plánů obnovy Objednatele.

Objednatel předpokládá, že bude zajišťovat obnovu systému do úrovně běžícího operačního systému. Zhotovitel pak odpovídá za obnovu aplikací, databází a úložiště dokumentů.

## Provozní monitoring

Pro Monitoring technické infrastruktury, aplikace a stavu dostupnosti služeb IT prostředí a Systému využívá Objednatel dohledový systém Zabbix v nejnovější verzi. Poskytovatel poskytne všechny podklady pro nastavení Monitoringu tak, aby byly monitorovány všechny nezbytné parametry pro sledování dostupnosti dodaného Systému dle Servisní smlouvy a predikcí problémů.

Současně Poskytovatel připraví testovací scénáře pro Monitorování základních uživatelských operací, které bude možno spouštět a vyhodnocovat pomocí dohledového systému tak aby bylo možno monitorovat stav dostupnosti a rychlosti odezvy jednotlivých operací Systému.

Dohledový systém umožňuje zasílání alertů emailem a SMS zprávami.