

Příloha č. 2 Výzvy



— **Bližší specifikace předmětu plnění  
(Technická specifikace)**

## Obsah

|       |   |    |
|-------|---|----|
| 1     | Seznam pojmů a zkratk .....   | 2  |
| 2     | Úvod .....  | 5  |
| 2.1   | Očekávání od DLP řešení .....   | 5  |
| 2.2   | Předmět plnění veřejné zakázky .....  | 6  |
| 2.3   | Oblasti, které nejsou předmětem plnění veřejné zakázky .....  | 7  |
| 3     | Současný stav a popis prostředí .....   | 7  |
| 4     | Požadavky na plnění .....   | 7  |
| 4.1   | Požadavky na navrhované DLP řešení.....   | 7  |
| 4.1.1 | Funkční požadavky.....  | 7  |
| 4.1.2 | Nefunkční požadavky.....  | 8  |
| 4.2   | Před-implementační analýza .....  | 8  |
| 4.2.1 | Předmět akceptace fáze Před-implementační analýza .....   | 9  |
| 4.3   | Implementace DLP řešení .....   | 10 |
| 4.3.1 | Předmět akceptace fáze Implementace DLP řešení .....  | 10 |
| 4.4   | Konfigurace a testování DLP řešení .....  | 10 |
| 4.4.1 | Předmět akceptace fáze Konfigurace a testování DLP řešení .....   | 11 |
| 4.5   | Adopce DLP řešení a školení administrátorů .....  | 12 |
| 4.5.1 | Předmět akceptace fáze Adopce DLP řešení a školení administrátorů ....                                  | 12 |
| 4.6   | Post-implementační podpora nově nasazených komponent do infrastruktury<br>SŽ a služby na vyžádání ..... | 12 |
| 5     | Fáze dodávky a akceptační milníky .....   | 13 |

## 1 Seznam pojmů a zkratek

Níže uvedená tabulka obsahuje seznam zkratek a pojmů použitých v rámci této Technické specifikace.

Přehled zkratek a pojmů:

| Zkratka                          | Popis   |
|----------------------------------|---|
| Agent-based                      | DLP řešení založené na agentech   |
| Agentless                        | DLP řešení bez instalace agentů na každé zařízení v síti  |
| AS-IS                            | Stav v současnosti, zpravidla architektury, prostředí, informačního systému apod.                                 |
| DLP                              | Řešení prevence úniku dat používaná zejména v rámci NGFW ( <i>Data Loss Prevention</i> )                          |
| Dodavatel                        | Účastník, který bude vybrán SŽ, se stane Dodavatelem  |
| HTTP, DNS, SNMP, SMTP, FTP, TFTP | Komunikační protokoly   |
| HW                               | Hardware  |
| ICT                              | Informační a komunikační technologie (Information and Communication Technologies)                                 |
| IS                               | Informační systém   |
| ISMS                             | Information Security Management System  |
| KII                              | Kritická informační infrastruktura  |
| LDAP, RADIUS, TACACS+, SAML      | Autentizační protokoly  |
| MD                               | Člověkodén, pracovní čas jedné osoby odpovídající jednomu pracovnímu dni, tedy typicky 8 hodin ( <i>Man-Day</i> ) |
| MPIP                             | Microsoft Purview Information Protection  |
| MS                               | Microsoft Corporation, americký výrobce především SW a provozovatel cloudového prostředí MS Azure                 |

|                |  |
|----------------|--|
| OCR            | Optické rozpoznávání znaků ( <i>Optical Character Recognition</i> )  |
| OS             | Operační systém ( <i>Operating System</i> )  |
| PTK            | Předběžná tržní konzultace je nástroj umožňující zadavateli veřejné zakázky oslovit dodavatele s požadavkem na informace ohledně zamýšlené připravované veřejné zakázky ( <i>Request for Information</i> )             |
| RBAC           | Řízení přístupů na základě rolí  |
| SaaS           | Software jako služba, je model poskytování SW uživatelům formou předplatného, kde veškerá odpovědnost za údržbu je na straně dodavatele. ( <i>Software as a service</i> )  |
| SIEM           | Řešení zabezpečení, které organizacím pomáhá detekovat bezpečnostní události, analyzovat je a reagovat na ně dříve, než způsobí škody v provozu firmy/organizace. ( <i>Security Information and Event Management</i> ) |
| SLA            | Smluvní nastavení záruk, úrovně, dostupnosti a kvality služeb atd. ( <i>Service-Level Agreement</i> )  |
| Smlouva o dílo | Smlouva o dílo – Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic. Závazný vzor Smlouvy o dílo je přílohou č. 3 Výzvy k podání nabídky              |
| SW             | Programové vybavení počítače či jiného obdobného zařízení. Speciálním druhem software je <i>firmware</i> , který je úzce spjatý s konkrétním hardwarem ( <i>Software</i> )   |
| SŽ             | Správa železnic, státní organizace („Zadavatel“)   |
| TDS            | Technologické datové sítě SŽ, jedná se o více VRF zpravidla vyhrazených pro OT, běžně se v prostředí SŽ nazývají také „Techlan“  |
| UAS            | Logická uživatelsko-aplikační síť SŽ, zahrnuje VRF v MPLS sítích a lokální VLAN, běžně se nazývá také „Intranet SŽ“  |
| Účastník       | Subjekt, který se účastní tohoto výběrového řízení o realizaci veřejné zakázky s názvem „Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic“          |

|      |  |
|------|--|
| VZ   | Veřejná zakázka „Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic“  |
| VoKB | Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů |
| ZoKB | Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů  |

## 2 Úvod

Tento dokument je přílohou a nedílnou součástí Výzvy k podání nabídky na veřejnou zakázku s názvem „Zavedení komplexního síťového řešení prevence úniku dat (DLP) pro non-Microsoft systémy v prostředí Správy železnic“, pro organizaci Správa železnic (SŽ). Dokument popisuje technické a jiné požadavky na veřejnou zakázku.

V rámci výběrového řízení je poptáváno provedení analýzy dat ve vyjmenovaných informačních systémech, dále ve spolupráci se SŽ určení klasifikace dat z těchto systémů a vytvoření knihovny detekčních signatur a reakčních pravidel pro detekci dat klasifikovaných jinak, než jako veřejná.

Dále je součástí poptávky návrh a implementace technických opatření pro zajištění prevence úniku dat v rámci prostředí SŽ. Tato opatření musí minimálně kontrolovat přenos dat mezi prostředím technologických sítí a uživatelskou sítí SŽ (interní perimetr) a mezi uživatelskou sítí a datovým provozem přecházejícím do veřejné sítě Internet (externí perimetr).

Navržené řešení nesmí modifikovat přenášená data jakýmkoliv způsobem, ani předpokládat jakoukoliv předchozí modifikaci dat (vyjma označení pomocí labelů s využitím nástroje Microsoft Purview Information Protection). Řešení dále nesmí ke své plné funkci vyžadovat běh jakýchkoliv lokálních agentů. Případné použití lokálních agentů pro rozšíření funkcionalit DLP řešení na individuálních zařízeních je akceptovatelné pouze po dohodě se Zadavatelem. Je však vhodné, aby DLP řešení umělo pracovat s již označenými daty konkrétně se štítky vytvořené nástrojem Microsoft Purview Information Protection.

Dodavatel zaškolí administrátory, kteří na systém budou přistupovat. Současně se školením Dodavatel vytvoří návrh adopční (komunikační) kampaně, která představí implementované změny uživatelům SŽ, tzn. jaký má systém účel a co pro ně jeho nasazení obnáší.

### 2.1 Očekávání od DLP řešení

SŽ očekává dosažení následujících cílů v rámci plnění veřejné zakázky:

- Snížení rizik v souvislosti s narušením parametru důvěrnosti pro definovaný rozsah citlivých dat.
- Identifikace citlivých dat v rámci specifikovaných systémů v prostředí SŽ a vytvoření pravidel pro jejich ochranu.
- Naplnění legislativních požadavků v kontextu ochrany citlivých dat v klíčových systémech.
- Automatizovaný přístup k detekci a zamezení úniku citlivých dat.
- Definování a nastavení způsobu reportingu detekovaných událostí, řešení incidentů a způsob úpravy detekčních a blokovacích pravidel.
- Předání know-how ohledně správy a konfigurace na interní tým SŽ pro správu řešení a politik, které vyžadují detailní znalost interního prostředí a pravidel pro nakládání s citlivými údaji.

- Definování detekčních pravidel a politik, které budou svým přístupem minimalizovat invazivní zásahy do činnosti uživatelů a systémů při dodržení zásad ochrany informací.

### Požadavky na rozsah řešení

Pro naplnění projektu ze strany Dodavatele je zapotřebí splnit následující:

- Vytvoření knihovny pravidel pro detekci klasifikovaných dat z vybraných systémů.
- Vytvoření knihovny signatur detekovaných dat.
- Ve spolupráci se Zadavatelem klasifikovat data v jednotlivých systémech.
- Zmapování toků dat z a do jednotlivých vybraných systémů.
- Návrh architektury řešení DLP (navržená architektura nesmí měnit celkovou cenu ani další hodnotící kritéria a musí být odsouhlasena Zadavatelem).
- Případná nová infrastruktura, potřebná pro DLP řešení, musí běžet ve virtualizované formě.
- Dodávka všech licencí potřebných k provozu navrhovaného DLP řešení.
- Implementace a konfigurace DLP řešení.
- Zaškolení vybraných zaměstnanců SŽ pro administraci a užívání DLP řešení.
- Vytvoření adopční kampaně pro zaměstnance SŽ.

## 2.2 Předmět plnění veřejné zakázky

Předmět plnění této veřejné zakázky je primárně založen na provedení analýzy a klasifikace informačních aktiv obsažených v systémech uvedených v rámci přílohy č. 8 Výzvy k podání nabídky s názvem – Informace k systémům SŽ z pohledu, a dále navržení, implementaci a konfiguraci DLP řešení do prostředí SŽ. Dodávka je rozdělena do následujících fází:

- Před-implementační analýza.
- Implementace DLP řešení do prostředí SŽ (v případě, že bude v rámci řešení využita).
- Konfigurace a testování nasazeného DLP řešení.
- Adopce řešení a školení administrátorů.
- Post-implementační podpora nově implementovaných komponent do infrastruktury SŽ.
- Služby na vyžádání.

Požadavky na tyto fáze jsou podrobně popsány v dalších částech tohoto dokumentu.

Součástí dodávky musejí být také dokumentace skutečného provedení, evidence nasazených pravidel a jejich garantů, včetně evidence použitých signatur s jejich popisem.

Dále musí být součástí dodávky veškeré případné licence pro plný běh DLP řešení.

Součástí plnění je i testování dodaného řešení. Jedná se hlavně o výkonnostní testy a testy účinnosti jednotlivých pravidel před zavedením do plného provozu. Testování musí probíhat tak, aby neomezilo nebo neohrozilo produkční systémy SŽ.

## 2.3 Oblasti, které nejsou předmětem plnění veřejné zakázky

Pro vyloučení pochybností SŽ uvádí, že následující oblasti **nejsou** předmětem plnění veřejné zakázky:

- Proxy servery či jiné zdroje dat pro DLP řešení.
- HW prostředky uvedené v rámci nabídky či jiné kapacity výpočetního výkonu (budou dodány ze strany Zadavatele). Dodavatel může maximálně požadovat celkový výpočetní výkon 160 jader a 768 GB RAM, kde jedna instance může být maximálně 128 jader a 512 GB, a zbylé instance pak maximálně 32 jader a 128 GB.
- Systém pro označování (štitkování) dokumentů a informací. Konfigurace IDS, IPS aj.

## 3 Současný stav a popis prostředí

Současný stav ICT prostředí, relevantní pro nasazení síťového DLP, je uveden v příloze č. 7 Výzvy k podání nabídky s názvem – Popis prostředí, kde jsou uvedeny základní informace k výchozímu stavu připravenosti prostředí SŽ pro nasazení řešení.

## 4 Požadavky na plnění

Plnění veřejné zakázky se musí skládat z níže uvedených fází:

1. Před-implementační analýza.
2. Implementace DLP řešení do prostředí SŽ (v případě, že bude v rámci řešení využita).
3. Konfigurace a testování DLP řešení.
4. Adopce DLP řešení a školení administrátorů.
5. Post-implementační podpora nově implementovaných částí DLP řešení a služby na vyžádání.

### 4.1 Požadavky na navrhované DLP řešení

Navrhované DLP řešení musí minimálně splňovat následující požadavky:

#### 4.1.1 Funkční požadavky

- Inspekce přenášených dat, a to minimálně protokoly HTTP, DNS, SNMP, SMTP, FTP, TFTP, Telnet (s již odstraněným šifrováním).
- Na externím perimetru jsou definovány signatury na základě finger print, regex slovník. Systém musí být schopen pracovat s českým jazykem. Na interním perimetru stačí definice signatur na úrovni regex.
- Dešifrování provozu šifrovaného pomocí TLS, minimálně ve verzích 1.2 a 1.3 a jejich následná inspekce, viz výše.
- DLP řešení musí podporovat autorizaci uživatelů pomocí rolí (tzv. RBAC)
- Rozdělení přístupových rolí minimálně na:



- Pouze náhled, pouze editace pravidel, plný administrátor.
- Řešení musí být schopno se napojit na externí poskytovatele identit, minimálně na Active Directory, Entra ID.
- Řešení musí podporovat minimálně následující autentizační protokoly - LDAP, RADIUS, TACACS+, SAML, Kerberos.
- Dodané řešení musí poskytovat možnost zapnutí vícefaktorové autentizace.
- Řešení musí logovat události, minimálně v rozsahu uvedeném v § 22 VoKB.
- Řešení musí být schopno odesílat logovací záznamy na vzdálený server pomocí protokolu Syslog ve formátu CEF nebo LEEF 2.0.
- V případě detekce musí být schopno minimálně následujících reakcí:
  - Nahlásit sepnutí pravidla
  - Změnit, nebo vymazat citlivý obsah
  - Zablokovat přenos dat.
- Řešení musí být schopno odesílat záznam bezpečnostní události o sepnutí pravidla do systému SIEM, nebo Log management systému, a to minimálně pomocí protokolu Syslog. Součástí události musí být minimálně jednoznačná identifikace zdrojového a cílového zařízení, identifikace detekčního pravidla, které bylo sepnuto, časová známka, data, která způsobila sepnutí pravidla a reakce systému.
- Na externím perimetru musí DLP řešení disponovat OCR.

#### 4.1.2 Nefunkční požadavky

- Nesmí být omezena propustnost linky (min. propustnost stejná jako kapacita linky, tj. 7x 1 Gb/s a 1x 2 Gb/s na interním perimetru a 1x 5 Gb/s na externím perimetru).
- Musí běžet v módu HA, nebo v módu, kdy v případě výpadku není nijak omezena komunikace na síti.
- Řešení nesmí běžet plně v cloudovém prostředí, minimální forma musí být hybridní režim, kdy část systému DLP běží na lokální infrastruktuře Zadavatele a pro pokročilé funkce rozpoznání dat, které neodpovídají žádné ze zavedených signatur, může být využito cloudové prostředí.
- Datové centrum hostující případnou část řešení musí být na území EU.
- V případě využití open source komponent je nutné prokázat zasmluvněnou platnou podporu vývojáře a zavázat se k jejímu nákupu na minimálně dalších 5 let, nebo prokázat správou vlastní vývojové větve po dobu minimálně 5 let a její využití v jiných dodávkách s hodnotou min. 2 000 000,- Kč bez DPH.

## 4.2 Před-implementační analýza

Cílem před-implementační analýzy je popsat minimálně následující oblasti:

- Analýzu dat v rámci jednotlivých vybraných systémů a ve spolupráci se Zadavatelem jejich klasifikace.
- Analýzu toku dat z a do jednotlivých vybraných systémů a identifikace možných cest úniku dat, které nelze pokrýt stávajícími technologiemi SŽ.
- Vytvoření knihovny signatur pro detekci dat v rámci DLP klasifikovaných jinak než veřejná, včetně popisu jednotlivých signatur.

- Vytvoření knihovny pravidel, pro reakce na detekovaná data nasaditelná do DLP řešení.
- Analýzu aktuálně nasazeného systému Microsoft Purview, nasazovaných štítků a pravidel. Analýza by měla odhalit případné kolize provozu nezávislých DLP řešení.
- Dále pak součástí návrhu musí být dokumentované řešení případných nalezených kolizí se systémem MS Purview Information Protection (MPIP). Navržená architektura by měla klást důraz na co nejlepší spolupráci systémů již provozovaných v prostředí SŽ, a pokud je to žádoucí, i jejich vzájemnou integraci (např. využití štítků z MPIP).
- Nezbytnou součástí této fáze je pak vznik detailního harmonogramu dalších fází a z toho vycházející seznam předpokládaných požadavků na součinnost ze strany Dodavatele.
- Předložení testovacích scénářů a jejich schválení ze strany Zadavatele. Zadavatel se zároveň zavazuje dodat připravené sady testovacích dat nejpozději v den před plánovaným testováním (viz dodaný harmonogram).
- Předložení návrhu architektury. Navrhovaná architektura nesmí navyšovat cenu ani HW prostředky (CPU a RAM), které byly indikovány v rámci nabídky ve výběrovém řízení. Součástí návrhu architektury musí být detailní rollback scénář, popisující odstranění jednotlivých změn provedených na infrastruktuře SŽ a její uvedení do původního stavu před začátkem implementace nebo konfigurace DLP řešení.

#### 4.2.1 Předmět akceptace fáze Před-implementační analýza

Předmětem akceptace této fáze je následující:

- Dokument zahrnující analýzu dat z vybraných systémů, obsahující minimálně popis vystupujících dat, jejich klasifikaci a šablony pro detekci.
- Dokument obsahující analýzu nasazení síťového DLP do prostředí s nasazeným MS Purview Information Protection. Analýza musí obsahovat identifikaci možných kolizí systémů a jejich odstranění a návrhy pro lepší spolupráci obou systémů.
- Dokument obsahující analýzu datových toků z a do vybraných informačních systémů s identifikací míst, která nejsou pokryta ochranou síťového DLP.
- Dokument obsahující katalog pravidel pro implementaci a jejich popis.
- Dokument obsahující detailní harmonogram implementace.
- Dokument obsahující seznam předpokládaných požadavků na součinnost Zadavatele.
- Dokument obsahující testovací scénáře.
- Dokument obsahující návrh architektury řešení.

Akceptace probíhá v souladu s dokumentem Zvláštní obchodní podmínky pro Zakázky v oblasti ICT (viz Příloha č. 5 Přílohy č. 3 Výzvy k podání nabídek (Závazný vzor smlouvy)

- Zvláštní obchodní podmínky pro Zakázky v oblasti ICT).

## 4.3 Dodávka licencí

- Dodávka všech licencí potřebných k provozu navrhovaného DLP řešení, minimálně po dobu 5 let od akceptace fáze F6 a F7 ze strany SŽ (viz Příloha č. 4 Výzvy k podání nabídky s názvem – Harmonogram plnění).

### 4.3.1 Předmět akceptace fáze Dodávka licencí

- Potřebné licence k provozu navrhovaného DLP řešení pro plný běh v rámci SŽ, minimálně po dobu 5 let od akceptace fáze F6 a F7 ze strany SŽ.

Akceptace probíhá v souladu s dokumentem Zvláštní obchodní podmínky pro Zakázky v oblasti ICT (viz Příloha č. 5 Přílohy č. 3 Výzvy k podání nabídek (Závazný vzor smlouvy) - Zvláštní obchodní podmínky pro Zakázky v oblasti ICT).

## 4.4 Implementace DLP řešení

Tato fáze závisí na návrhu DLP řešení. V případě, že navrhované DLP řešení nevyžaduje implementaci nové infrastruktury do prostředí SŽ a vystačí si s nástroji, které má SŽ již k dispozici, nebude tato fáze ze strany Dodavatele využita.

V opačném případě je v rámci této fáze nutné nasadit celé navrhované DLP řešení do infrastruktury SŽ a napojit ho na požadované zdroje dat, případně další nezbytnou infrastrukturu (NTP, identitní databáze aj.).

### 4.4.1 Předmět akceptace fáze Implementace DLP řešení

Předmětem akceptace této fáze je následující (pokud bude využita ze strany Dodavatele):

- Kompletně nasazené DLP řešení do infrastruktury SŽ (má k dispozici všechny specifikované funkcionality, má napojeny všechny zdroje dat a veškeré další vyžadované činnosti jsou pouze konfiguračního charakteru).
- Nasazeným DLP řešením musí procházet všechna data, která jsou v rámci analýzy identifikována jako data, která je zapotřebí monitorovat a data překračující jeden z určených perimetrů (interní, externí).

## 4.5 Konfigurace DLP řešení

Tato fáze obnáší hlavně nasazení vyspecifikovaných pravidel a konfiguraci řešení pro jejich plné fungování a maximální efektivitu. Konečná konfigurace musí zvládnout dešifrovat provoz šifrovaný protokolem SSL/TLS ve verzích minimálně 1.2 a 1.3. Musí také umět odhalit klasifikovaná data, minimálně v protokolech HTTP, DNS, TFTP, SMTP, SNMP, FTP, TFTP a Telnet.

#### 4.5.1 Předmět akceptace fáze Konfigurace DLP řešení

Předmětem akceptace této fáze je následující:

- Dokument popisující stav skutečného provedení. Dokument musí obsahovat aktuální architekturu systému a popis předávané konfigurace systému se zachycením všech aktuálních schopností systému (ne pouze minimálního rozsahu).
- Systém, který je plně nakonfigurovaný a připravený k otestování ze strany SŽ a následně připraven k ostrému spuštění. Součástí i je zavedení potřebných uživatelů, přidělení oprávnění a předání administrátorských účtů zástupcům SŽ atd.

Akceptace probíhá v souladu s dokumentem Zvláštní obchodní podmínky pro Zakázky v oblasti ICT (viz Příloha č. 5 Přílohy č. 3 Výzvy k podání nabídek (Závazný vzor smlouvy) - Zvláštní obchodní podmínky pro Zakázky v oblasti ICT).

#### 4.6 Testování DLP řešení

V rámci této fáze také proběhne otestování funkčních schopností DLP řešení a detekčních schopností každého z nasazených pravidel.

Po otestování funkčnosti jednotlivých pravidel musí proběhnout zátěžové testy k ověření celkové konfigurace, viz akceptační kritéria.

##### 4.6.1 Předmět akceptace fáze Testování DLP řešení

- Úspěšné otestování dekrypce provozu.
- Úspěšné otestování schopnosti detekce všech nasazených pravidel (každé pravidlo musí úspěšně detekovat informace, pro jejichž detekci bylo vytvořeno na základě dokumentace pravidla. Data pro testování budou poskytnuta ze strany SŽ). Otestování funkčnosti pravidla proběhne na všech protokolech vyjmenovaných v dokumentaci skutečného provedení, ve kterých má nástroj schopnost zachytu.
- Úspěšně provedené výkonnostní testy (systém musí zvládnout zpracovat min. 1 Gb/s na každém prostupu interního perimetru, v případě agregovaných linek pak součet kapacit těchto agregovaných linek a min. 5 Gb/s dat na externím perimetru).
- Úspěšně provedené testy výpadku DLP řešení.

Testování provede SŽ nebo subjekt, který bude určen ze strany SŽ.

#### 4.7 Testovací provoz

Po ověření funkčnosti v rámci F5 bude následovat tříměsíční testovací provoz. Nálezy vzešlé z tohoto testovacího provozu musejí být následně, nebo ještě v době testovacího provozu, odstraněny.

##### 4.7.1 Předmět akceptace fáze Testovací provoz

- Vypořádání všech nálezů vzniklých v rámci testovacího provozu

Akceptace probíhá v souladu s dokumentem Zvláštní obchodní podmínky pro Zakázky v oblasti ICT (viz Příloha č. 5 Přílohy č. 3 Výzvy k podání nabídek (Závazný vzor smlouvy) - Zvláštní obchodní podmínky pro Zakázky v oblasti ICT).

## 4.8 Adopce DLP řešení a školení administrátorů

Adopční část fáze spočívá ve vytvoření adopční kampaně pro zaměstnance SŽ. Adopční kampaň bude složena z pětiminutového videa a informačního emailu. Adopční kampaň má za účel informovat zaměstnance SŽ o účelu systému, jeho schopnostech a vlivu na práci zaměstnanců.

Školení zahrnuje:

- Školení administrátorů řešení v celkové délce školení 16 hodin (maximálně 25 účastníků).
- Účast na školení musí být stvrzena prezenční listinou.
- Všechna školení proběhnou v prostorách SŽ za přítomnosti školitele/školitelů Dodavatele v hybridním režimu (osobně, s možností vzdáleného přístupu), ze všech školení bude pořízen video záznam pro potřeby dalšího školení pracovníků SŽ.

### 4.8.1 Předmět akceptace fáze Adopce DLP řešení a školení administrátorů

Předmětem akceptace této Fáze je následující:

- Dokument (formátu informačního posteru) a video soubor (cca 5 min) pro adopční kampaň.
- Provedení školení administrátorů.

## 4.9 Post-implementační podpora nově nasazených komponent do infrastruktury SŽ a služby na vyžádání

Součástí dodávky bude i pětiletá podpora na celkové řešení vyjma komponent, které jsou již aktuálně součástí infrastruktury SŽ a aktuálně spadají pod smlouvu o podpoře. Podpora, která bude poskytována po ukončení fáze 3.5 (viz Příloha č. 4 Výzvy k podání nabídky s názvem - Harmonogram plnění), bude zahrnovat SLA na případně vyskytující se chyby a pravidelnou profylaxi celého řešení jednou za 3 měsíce. Součástí podpory jsou dále pravidelné upgrady systému a aplikace bezpečnostních patchů (či mitigace zranitelnosti), a to nejpozději do týdne od vydání výrobcem, a u kritických zranitelností nejpozději do 24 hodin po vydání patche, nebo mitigace.

Dodavatel poskytne SŽ služby na vyžádání, přičemž půjde o služby dvojího charakteru, což vyplývá z tabulky uvedené níže. Maximální souhrn těchto služeb bude činit 30 MD za celou dobu trvání smlouvy, čerpání bude probíhat dle konkrétních potřeb SŽ.

SŽ požaduje uvést cenu za následující položky ve formě ceny za 1 MD a celkové ceny za položku podle předpokládaného objemu čerpání:

| Položka  | Předpokládané čerpání v MD |
|--|----------------------------|
| Služba konzultační technické podpory dodaného řešení (technické a metodické otázky související s provozem a rozvojem řešení) | 20                         |
| Změnová řízení, zakázkový vývoj, doplnění řešení   | 10                         |

Celková cena za výše uvedené položky musí být součástí cenové nabídky Dodavatele. SŽ není povinna služby na vyžádání čerpat.

## 5 Fáze dodávky a akceptační milníky

Dodávka má být dodána v níže uvedených fázích. Každá z níže uvedených fází musí být SŽ separátně akceptována nejpozději v termínu uvedeném v Harmonogramu, s výjimkou F8, kde post-implementační podpora bude akceptovaná na bázi měsíčních výkazů práce a akceptace služeb na vyžádání bude specifikována v rámci konkrétních objednávek. SŽ akceptuje výstupy dané Fáze, jestliže je Dodavatel provedl v šíři a kvalitě požadované v zadávacích podmínkách této veřejné zakázky. V opačném případě je Dodavatel povinen napravit nedostatky dodávky.

| Fáze      | Popis   |
|-----------|---|
| <b>F1</b> | Fáze Před-implementační analýza   |
| <b>F2</b> | Fáze Dodávka licencí  |
| <b>F3</b> | Fáze Implementace DLP řešení (pokud bude ze strany Dodavatele využito)                              |
| <b>F4</b> | Fáze Konfigurace DLP řešení   |
| <b>F5</b> | Testování DLP řešení  |
| <b>F6</b> | Testovací provoz  |
| <b>F7</b> | Fáze Adopce DLP řešení a školení administrátorů   |
| <b>F8</b> | Fáze Post-implementační podpora nově nasazených komponent do infrastruktury SŽ a služby na vyžádání |