PŘÍLOHA Č. 1 KE KUPNÍ SMLOUVĚ

TECHNICKÁ SPECIFIKACE

Nemocnice Rudolfa a Stefanie Benešov, a.s.

safetica®

POPIS ŘEŠENÍ

Software Safetica je kompletní řešení vnitřní bezpečnostní, které přináší změnu ve vnímání rizik. Zatímco ostatní hovoří o datech a ochraně soustředěné na data, my chápeme, že data neunikají ze společnosti sama od sebe.

Software Safetica nabízí ucelené řešení prevence úniku dat (DLP) pokrývající hrozby se společným původcem – selháním lidského faktoru. Důkladný přístup tohoto řešení zahrnuje velkou paletu bezpečnostních nástrojů, z nichž každý by vyžadoval samostatné aplikace od několika výrobců.

Ihned po nasazení nabízí Safetica silné DLP řešení zahrnující ochranu dat a informování managementu o hrozících rizicích. Safetica také nabídne možnost vymezit aktivitu personálu tak, aby odpovídala bezpečnostním politikám vaší společnosti.

Jak Vás Safetica ochrání?

Software Safetica se soustředí na ochranu na vyšší úrovni – zaměřuje se na eliminaci zdrojů hrozeb. A za každým ohrožením dat stojí osoba za tento incident zodpovědná, ať již úmyslně nebo nedbalostí.

Důvody úniku dat, se kterými se firmy setkávají nejčasteji, jsou:

- Omyly při posílaní souborů
- Kopírování na osobní zařízení
- Krádež/ztráta zařízení (notebook, pevný disk, tablet, mobil)
- Upload na cloudové úložiště
- Rizika BYOD
- Vydíraní a podvody

Hlavní výhody Safetica

Software Safetica chrání vaši společnost před následky úniků citlivých informací a ztrátami spojenými s neefektivně vynaloženými personálními náklady. Je to jediný software, který šetří váš čas a peníze včasnou identifikací nebezpečného chování.

Safetica eliminuje všechny neúmyslné chyby ale i záměrné snahy o poškození vaší společnosti. Vyznačuje se snadnou implementací, díky které rychle získáte plnohodnotné bezpečnostní řešení.

Safetica pokrývá všechny cesty úniků dat. Citlivé dokumenty zůstanou chráněny před nepovoleným kopírováním, odesláním e-mailem anebo tiskem.

Rychlá implementace. Univerzální přístup k blokování aplikací a cest úniků dat umožňuje nejrychlejší nasazení mezi dostupnými DLP nástroji

Vysoká ochrana proti obejití, včetně ochrany před uživateli s administrátorskými právy.

Univerzální přístup. Safetica se nesoustředí pouze na několik vybraných aplikací nebo typů souborů. Ochrana dat probíhá u všech aplikací, typů dat nebo síťových protokolů (včetně těch šifrovaných).

Čistě definovaná bezpečnostní pravidla díky Bezpečným zónám. Jednoduše nastavíte perimetr, za který data nesmí a Safetica se postará o bezpečnost těchto dat.

Přesné sledování času. Spuštění aplikace nebo otevření souboru ještě neznamená aktivní používání. Safetica zaznamenává a ukazuje čas, kdy uživatel skutečně pracoval se souborem, aplikací, nebo webem.

Automatické reporty a upozornění. Safetica vyhodnotí nejdůležitější zaznamenané aktivity a pošle zprávu zodpovědnému manažerovi.

Jedno místo pro správu. **Safetica umožňuje řešit bezpečnost centrálně,** z jednoho místa lze získat informace o incidentech i nastavovat bezpečnostní pravidla.

Online analytický nástroj pro manažery, **WebSafetica, přehledným způsobem umožňuje zjistit, co se děje ve vaší organizaci.** Běží v každém prohlížeči, na počítači i mobilu. Díky tomu můžete zkontrolovat firemní bezpečnost i z pohodlí domova.

Minimální náklady na implementaci a provoz (nízké TCO)

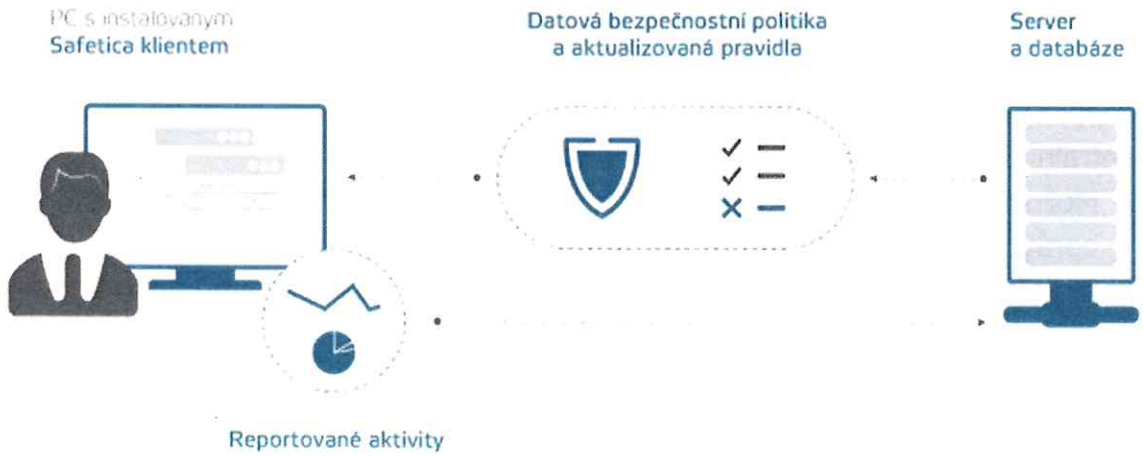
Klíčové funkce Safetica

Kompletní audit pohybu dat a činnosti uživatelů	Získejte úplný přehled o tom, které aktivity ve vaší organizaci jsou potenciálně riskantní. Navíc celý souhrn o zabezpečení můžete dostávat jako pravidelný email do vaší schránky.
Kompletní prevence úniku dat	Safetica zabezpečí všechny cesty proti úniku dat. Instaluje se rychle a zobrazí bezpečnostní rizika srozumitelným způsobem.
Testovací a informativní DLP režimy	Safetica umožňuje testovací režim, ve kterém vyzkoušíte chod ve vaší firmě bez jakýchkoliv zásahů do provozu. Poté můžete spustit informativní režim, který umožňuje vzdelávat uživatelé o nových pravidlech pro zabezpečení citlivých dokumentů.
Analýza trendů a produktivity	Software varuje vedení společnosti v případě náhlých změn v chování zaměstnanců nebo při dlouhodobém poklesu produktivity. Safetica odhalí porušení bezpečnostních nařízení a upozorní na možné hrozby dříve, než jsou citlivé informace skutečně ohroženy.
Blokování aplikací a webů	Můžete také jednoduše vybrat, která skupina pracovníků má přístup k jakým webovým stránkam. Blokovat můžete konkrétní servery nebo vytvářet pravidla na základě kategorií.
Snížení nákladů správou tisku	Safetica kontroluje, kdo může tisknout jaké dokumenty. Získáte tak přehled o efektivitě tisku ve vaší firmě.

Správa externích zařízení	Safetica zamezí uživatelům v připojování zařízení, které nejsou schválena pro provoz ve firemní síti.
Šifrování počítačů a externích zařízení	Se Safetica můžete zašifrovat důležité dokumenty, USB disky nebo rovnou obsah celého počítače, takže se nikdo nepovolaný nedostane k citlivému obsahu.
Safetica Mobile	Zabezpečte tablety a mobilní zařízení proti ztrátě či krádeži a spravujte všechny firemní počítače a mobily na jednom místě.
Inspekce šifrovaných spojení SSL/HTTPS	Safetica kontroluje také zabezpečená spojení k webovým stránkám, šifrované IM spojení a zabezpečené e-mailové přenosy.

Jak Safetica funguje?

Většina práce s daty se odehrává na koncových stanicích: Uživatelé zde pracují s citlivými informacemi, tisknou je, přistupují na internet, připojují přenosná média nebo posílají e-maily. Na každé stanici v síti je instalován Safetica klient, který udržuje pravidelný kontakt se serverem a databází, posílá informace o dění a incidentech a stahuje si nové nastavení.



Zabezpečení na koncové stanici

Reportování aktivit:

- Všechny operace se soubory včetně podpory RDP a cloudových disků
- Dlouhodobé trendy, krátkodobé odchylky v aktivitách
- Webové stránky (všechny prohlížeče včetně HTTPS a záznamu délky aktivity)
- E-maily (SMTP, POP3, IMAP, Microsoft Outlook/ MAPI protokoly)
- Využiti aplikací včetně aktivního a neaktivního času
- Virtuální, lokální i síťové tiskárny
- Využití počítačů a sítě
- Podpora terminálových serverů

Prevence úniků dat:

- Pevné disky, USB, CD/DVD, FireWire, SD/MMC/CF karty, Bluetooth a další
- Přenos souborů po síti (zabezpečený i nezabezpečený) – HTTPS/SSL
- E-maily (SMTP, POP3, IMAP, Microsoft Outlook/ MAPI protokoly)
- Detekce a restrikce Cloudových disků
- Upload a download přes webové prohlížeče
- Šifrování lokálních a externích disků
- Kopírování přes schránku, drag & drop přetažení
- Virtuální, lokální i síťové tiskárny
- Kontrola přístupu aplikací k souborům
- Vytvoření snímku obrazovky

Podrobná funkcionalita splňující požadavky dle zadání:

Obecné

- Integrace s Microsoft® Active Directory®
- Podpora databázového serveru MS SQL 2008, 2008 R2 nebo 2012
- Podpora OS Windows XP a vyšší vč. Vista, 8/8.1, 10
- Podpora OS Windows Server 2008, R2, 2012
- Podpora terminálového prostředí
- Centrální administrativní konzole s přizpůsobením
  - Možnost auditu přístupu k výsledkům a nastavením produktu, řízení přístupových oprávnění k administraci
- Skrytý režim vč. skrytí procesu a složek, a to i vzhledem k lokálnímu nebo doménovému administrátorovi přítomnému na koncové stanici
- Ochrana proti obejití systému
  - Ochrana systému proti obejití musí být aktivní pro uživatele, lokálního i doménového administrátora
  - Nemožnost zastavit procesy, v případě zvýšených práv automatické obnovení nebo jiná ochrana
  - Nemožnost odinstalace bez explicitní autorizace
  - Nemožnost změny registru, zásahu do komponent systému, knihoven DLL

  - Nemožnost měnit nastavení z koncové stanice
  - Musí existovat řešení pro ochranu v nouzovém režimu (safe mode)
- Funkčnost musí přetrvat také v tzv. offline režimu mimo připojení do firemní sítě nebo na internet
- Možnost práce s historickými daty
- Řešení musí podporovat nebo přímo poskytovat zálohování vlastních komponent, zejména záznamů a konfigurace
- Generování automatických emailových zpráv v případě vzniku incidentu, lze přizpůsobit prahy citlivosti i specifikaci incidentu
- Generování automatických reportů do emailu, tyto lze plně přizpůsobit (jaké informace, za jaké uživatele, jak často a komu budou přicházet)
- Možnost posílání záznamů do SIEM systému
- MDM řešení pro Android, iOS a Windows Phone

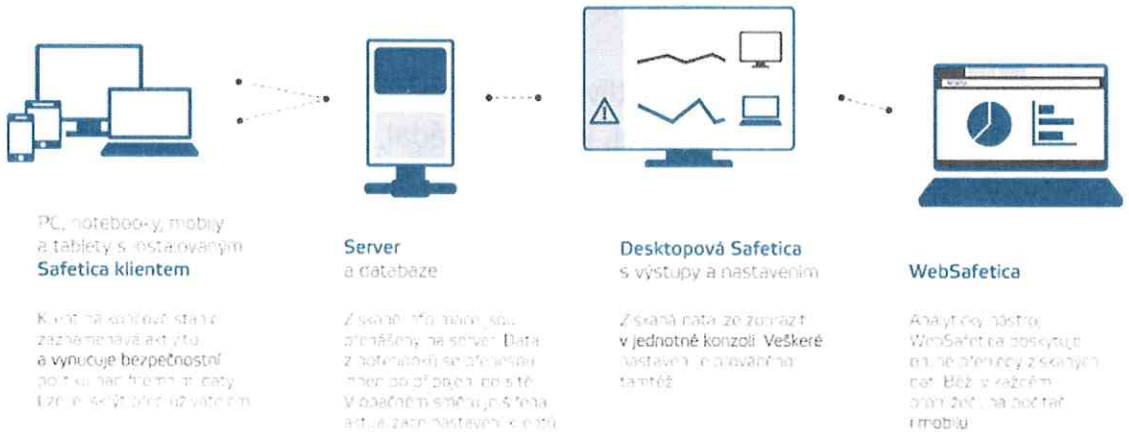
Bezpečnostní audit

- Obecně:
  - podrobné informace o době spuštění a rovněž o době skutečně aktivního využívání konkrétních aplikací, tyto jsou zároveň pro rychlé vyhodnocení tříděny do kategorií
  - Informace o skutečně aktivním čase jednotlivých webových stránek, včetně podrobných informací o URL, protokolu a titulku okna, nezávisle na použitém prohlížeči, tyto jsou zároveň pro rychlé vyhodnocení tříděny do kategorií
  - Možnost exportu záznamů do XLS, PDF
- Instant Messenger aplikace, webový email – možnost monitorování nezávisle od typu aplikace nebo služby
- E-mail:
  - Podpora protokolů POP3, IMAP, MAPI / Exchange vč, šifrování SSL
  - Podpora emailového klienta MS Outlook, Thunderbird, Icewarp,.... – řešení je schopné monitorovat e-mailové aplikace, nezávisle na typu aplikace
- Pohyb dat:
  - podrobné informace o práci s citlivými soubory jako kdo k těmto přistupoval, v jakých aplikacích s nimi pracoval, kam je ukládal, přejmenování a mazání, včetně externích zařízení, emailů a cloudových úložišť vč. synchronizované složky na disku
  - Lokální operace se soubory – kopírování, přesun, stažení z webu, FTP, mazání, vytváření, otevírání včetně identifikace zdrojové a cílové lokality – cesta, typ zařízení, jednoznačný identifikátor
  - Logování vytištěných dat
  - Použití kopírování do schránky a snímání obrazovky
- Aktivita na stanici:
  - Log zapnutí/vypnutí PC
  - Log přihlášení/odhlášení uživatele
  - Log spánku/vzbuzení PC
- Síťová aktivita:
  - Objem stažených a zaslaných dat

Ochrana dat

- **Obecně:**
  - Nezávislost na aplikaci, protokolu vč. šifrovaného spojení
  - Řešení je odolné vůči obejití ochrany na souborovém systému při použití odkazů na jiné složky včetně symbolických odkazů a podobných technologií
- **Šifrování:**
  - Šifrování celých disků (Full Disk Encryption) i pro systémové disky
  - Šifrování souborů
  - Virtuální šifrované disky
  - Vynucení šifrování v předem definovaných akcích (zasílání dat na neautorizovaná úložiště)
- **Data Loss Prevention**
  - Pro určené kategorie citlivých dat mít možnost omezit pohyb a práci s daty – které média mohou být použity pro přenos, na jaký web může být provedeno nahrání souboru, na jakou emailovou adresu mohou být data zaslána; jaká aplikace může data otevřít
  - Možnost monitorovacího, upozorňovacího i zakazovacího režimu
  - Možnost navázání politik na konkrétní aplikace – definice zdrojů (konkrétní data, přístup k externím zařízením, síti), které aplikace může využít pro svůj běh
- **Device Control**
  - Globální omezení na USB, firewire, mobilní telefony, paměťové karty, LPT, COM, Bluetooth, CD, DVD, Blue-ray
  - Možnost read-only módu
  - Auditní záznam veškerých externích zařízení připojovaných do systému vč. monitoru, klávesnic a myši

Architektura řešení



Doporučené technické požadavky

Safetica klient:

- 2,4 GHz dvoujádrový procesor
- 2 GB paměti RAM
- 10 GB volného místa na disku
- Instalace na koncové stanici
- MS Windows 7 a vyšší, 32-bit i 64-bit

Safetica server:

- 2 GHz dvoujádrový procesor (doporučujeme čtyřjádrový)
- 4 GB paměti RAM
- 20 GB volného místa na disku
- Instalace na aplikační nebo dedikovaný server (lze využít virtualizace)
- Podpora Active Directory
- MS Windows Server 2008 a vyšší, 32-bit i 64-bit
- Vyžaduje připojení k serveru s MS SQL 2008 R2 a vyšší
- Při sdílení s MS SQL minimálně čtyřjádrový procesor, 8GB RAM a 100GB volného místa na disku

MS SQL (databáze pro server):

- Požadavky dle edice MS SQL
- Sdílený nebo dedikovaný server, doporučujeme min. 100GB volného místa na disku
- MS SQL 2008 R2 a vyšší, případně MS SQL 2012 Express a vyšší (verze zdarma)
- MS SQL 2012 Express je volitelná součást instalátoru

Technická specifikace obecného nastavení (definice a ochrana bezpečného perimetru)

Auditor

Ponechání auditního nástroje ve výchozím stavu (všechny funkce monitorování zapnuty) za účely auditu datového toku a detekce potencionálně nebezpečných operací.

Supervisor

Preventivní omezení uživatelského přístupu k webům a aplikacím, které mohou způsobit únik dat.

- Správa webu:
    - Blokování kategorií: Games, Illegal, Pornography
- Správa aplikací:
    - Blokovaní kategorií: Keylogger, Alternative web browsers, Miners

Varování

Varování týkající se:

- přenosu velkého množství dat na externí zařízení
- nahrávaní velkého množství dat na web

- vyhledávaní práce

Reporty

Reportovat využívání nákladných aplikací uživateli a jejich následná optimalizace.

DLP

BitLocker

Využít správu BitLockeru, jenž je v konzoli Safetica dostupná a šifrovat nejen disky koncových stanic, ale také případná povolená externí paměťová zařízení.

Správce zařízení

Definování povolených zařízení a následné omezení jednotlivých portů počítače na režim „pouze pro čtení" nebo „Zakázat"

Hlídání disků

Omezení cloudových klientů, jenž nejsou spravovány zákazníkem. Optimalizace přístupů uživatelů do konkrétních lokálních či síťových cest. Následné přístupy do složek logovat.

OCHRANA CITLIVÝCH DAT KE VTAHU K GDPR

DLP – Zóny

Definování bezpečného perimetru pro nahrávání, ukládání a zasílání dat.

safetica

PŘÍLOHA Č. 2 KE KUPNÍ SMLOUVĚ

HARMONOGRAM

Nemocnice Rudolfa a Stefanie Benešov, a.s.

Harmonogram projektu

Fáze projektu	Předpokládané trvání	Časový předpoklad*
1. Instalace	1 týden od kick-off meetingu	-
2. Monitorovací období	1 týden od akceptace fáze 1	-
3. Analýza sesbíraných dat	Přibližně 1 týden od akceptace fáze 2	-
4. Školení	(součástí ostatních fází)	-
5. Konfigurace Simple DLP	1 týden od akceptace fáze 3	Do 26. 6. 2019
6. Konfigurace Advanced DLP	Dle zákazníka	-

*Údaje jsou orientační, jsou nastaveny od data zhotovení tohoto dokumentu, jejich reálné plnění se však bude odvíjet od data schválení tohoto dokumentu Objednatelem. Dodavatel si vyhrazuje po předchozí domluvě s Objednatelem právo na posun termínů, jejichž plnění se mimo jiné odvíjí i od součinnosti Objednatele.

Plánované ukončení projektu

V případě včasného naplnění jednotlivých fází projektu se uzavření projektu datuje na jeden měsíc od akceptace fáze 1, tedy 26.6. 2019.

Podmínky pro implementaci produktu

Objednatel je zodpovědný za zajištění následovných podmínek pro implementaci:

1. Zajistit splnění všech **hardwarových** a **softwarových** podmínek pro instalaci databáze Microsoft® SQL Server (2012 a vyšší), Safetica Management Service, Safetica Management Console, WebSafetica, Safetica Agent, Safetica Endpoint Client na relevantních stanicích z požadovaného rozsahu implementace dle přílohy 5 Smlouvy o dílo. Jednotlivé HW/SW požadavky služeb Safetica jsou uvedeny v dokumentu „Informace o nasazení" nebo „CZ Informace o POC"

2. Splnit povinnosti, které mu mimo jiné v souvislosti s nasazením produktu Safetica, **ochranou soukromí a zpracováním osobních údajů** ukládá Obecné nařízení o ochraně osobních údajů (GDPR) a 262/2006 Sb. (zákoník práce), a to nejpozději do data uzavření smlouvy o dílo k software Safetica. Doporučení k docílení shody produktu s požadavky regulace GDPR naleznete v následujícím dokumentu „Jak používat Safetica v souladu s GDPR"

3. Zajistit **vzdálený přístup a dostupnost k**:

- serverům, na kterých běží **služby Safetica Management Service, WebSafetica a Microsoft SQL Server s Windows účtem**, jenž bude mít **dostatečná oprávnění pro správu jednotlivých služeb Safetica a databází Safetica** (safetica_category, safetica_data, safetica_main)

- stanici nebo serveru s nainstalovanou administrátorskou konzolí **Safetica Management Console**

- **testovací stanici** (fyzická nebo virtuální) – reprezentující rozmanitost produkčního prostředí. Tato stanice bude následně sloužit k otestování kompatibility Safetica s ostatními relevantními produkty a případně ověření konfigurace Safetica DLP před přenesením do produkčního prostředí

4. Na všech stanicích, kde bude prováděna instalace Safetica Agent, **zajistit možnosti vzdálené nebo lokální instalace**

5. Pro případné řešení problémů **umožnit vzdálený přístup na stanice nebo zaručit plnou spolupráci při sběru ladících výpisů**

6. Zajistit spolupráci a **součinnost všech zainteresovaných osob** po celou dobu implementace

7. V případě ladění problémů zajistit **obeznámenost** všech odpovědných osob s postupy pro kontaktování zákaznické podpory Safetica Technologies, dle komunikační matice uvedené v části „Komunikační platforma"

8. V případě jakýchkoliv změn, které se týkají jak konfigurace nebo modifikace produktu či implementačního procesu, je **nutné** požadované **změny zaslat písemnou formou** a změna musí být před implementací **ze strany projektového manažera zhotovitele zaevidována a schválena**

1. Instalace

Cílem úvodní fáze implementace řešení Safetica je nasazení všech komponent do prostředí objednatele pouze v základním nastavení. Jednotlivé kroky jsou následující:

- Příprava serveru dle technických požadavků – ze strany objednatele

- Instalace či konfigurace databázového serveru

- Instalace serverové služby Safetica Management Service

- Instalace konzolí Safetica a WebSafetica

- Konfigurace úvodního průvodce nastavením produktu (nastavení SMTP serveru, vložení licenčního klíče, propojení s AD aj.)
- Nasazení komponenty Safetica Agent na všechny klientské stanice v rozsahu implementace.
    - Ruční instalace (například z USB zařízení, síťového disku)
    - Vzdáleně pomocí Microsoft Active Directory Group Policy
    - Využití produktů třetích stran
- Nasazení komponenty Safetica Client na koncové stanice prostřednictvím konzole Safetica v rozmezí:
    - 5 % koncových stanic, jenž reprezentují heterogenní prostředí objednatele
    - 25 % koncových stanic
    - 100 % koncových stanic
- Ověření sběru dat
- Instalace Safetica Mobile na mobilní zařízení, pokud jsou součástí implementace.

2. Monitorovací období

Cílem této fáze je sběr dat z koncových stanic pro analýzu pohybu dat, uživatelského chování a využití IT prostředků. Kroky pro tuto fázi jsou následující:

- Kontrola sběru dat v pravidelných týdenních intervalech
- Kontrola produktu

3. Analýza sesbíraných dat

Cílem této fáze je příprava výstupní analýzy z dat sesbíraných v rámci monitorovacího období, jejich strukturalizace, vizualizace a prozkoumání případných incidentů uživatelů na pracovišti. Výstupem je komplexní shrnutí, seznam rizik a doporučených opatření.

Kroky jsou následující:

- Kategorizace záznamů sesbíraných v rámci monitorování aplikačních a webových přístupů
- Definování pracovní doby, interních systémů
- Export zdrojových dat pro zpracování

- Příprava výsledné zprávy a detailních záznamů
- Prezentace analýzy s následnou konzultací nastavení
- Konzultace, připomínkování, finalizace a schválení předložených nastavení

4. Školení

Zodpovědné osoby objednatele budou zaškoleny pro práci s produktem. Tyto služby budou dodány v rámci ostatních fází dodávky díla. Trvání není přesněji definováno a odvíjí se od průběhu projektu. Po uzavření projektu jsou nové informace předávány v rámci údržby.

5. Konfigurace

Cílem této fáze je aplikace domluvených nastavení do konkrétního prostředí objednatele a potvrzení dodání ze strany implementátora na straně dodavatele a objednatele.

Kroky jsou následující:

- Konfigurace / úprava domluvených nastavení
- Zajištění kompatibility s interními systémy objednatele v případě rozšířených nastavení
- Vyhodnocení a optimalizace navržených nastavení

6. Uzavření

Cílem je formální potvrzení implementace produktu dle stanovených akceptačních kritérií.

Praha | Česká republika |

Příloha č. 3 kupní smlouvy

AKCEPTACE VÝSLEDKŮ POSKYTOVANÉHO PLNĚNÍ

1) Výsledky a výstupy prodávajícím poskytovaného plnění budou akceptovány kupujícím na základě příslušné akceptační procedury.

2) Řízení o akceptaci předaného plnění (nebo jeho části) je zahájeno dnem předání plnění podle smlouvy a je ukončeno podpisem akceptačního protokolu kupujícím a prodávajícím (dále jen „Akceptační protokol") v případě, že prodávajícím předané plnění (nebo jeho část) splňuje podmínky a vlastnosti stanovené smlouvou, je funkční, bez nedodělků bránicích užití plnění (nebo jeho části). Akceptační protokol bude obsahovat minimálně

   a) popis plnění nebo jeho části, které byly předmětem akceptace;

   b) záznam průběhu akceptačního řízení;

   c) seznam akceptačních testů se záznamem jejich výsledků;

   d) seznam zjištěných vad s jejich klasifikací dle kategorií;

   e) výsledek akceptačního řízení.

3) Kupující provede oponentní řízení převzatého plnění (nebo jeho části), a nejméně dva (2) pracovní dny před ukončením akceptačního řízení, které se koná v dohodnutém termínu, sdělí prodávajímu výhrady k předanému plnění s vyznačením jejich závažnosti. Na akceptačním řízení budou projednány výhrady kupujícího a stanovena výsledná závažnost připomínek, vad a nedodělků, včetně termínů jejich odstranění. Při stanovení výsledné závažnosti připomínek kupující vezme do úvahy stanovisko prodávajícího. Výsledky tohoto řízení budou uvedeny do Akceptačního protokolu.

4) Kategorizace vad předávaného plnění při akceptačním řízení:

   Vada kategorie A
   Popis vady: Vážné vady s nejvyšší prioritou, které mají kritický dopad do funkčnosti plnění nebo jeho části a dále vady, které znemožňují užívání plnění nebo jeho části kupujícím nebo způsobují vážné provozní problémy.
   Vada kategorie B
   Popis vady: Vada, která svým charakterem nespadá do kategorie A. Znamená však vážné vady způsobující zhoršení výkonnosti a funkčnosti plnění nebo jeho části. Plnění nebo jeho část má omezení nebo je částečně nefunkční. Jedná se o odstranitelné vady, které způsobují problémy při užívání a provozování plnění nebo jeho části kupujícím, ale umožňují provoz.
   Vada kategorie C
   Popis vady: Vada, která svým charakterem nespadá do kategorie A nebo kategorie B. Znamená snadno odstranitelné vady s minimálním dopadem na funkcionality či funkčnost plnění nebo jeho části.

5) Výsledkem akceptačního řízení mohou být tři (3) stavy:

   Akceptováno bez výhrad. V případě, že nebudou v průběhu akceptačního řízení zjištěny v předaném plnění (nebo jeho části) žádné vady ani nedodělky (dle výše uvedené kategorizace),

uvede kupující do Akceptačního protokolu, že předané plnění (nebo jeho část) bylo akceptováno bez výhrad a Akceptační protokol potvrdí svým podpisem.

Akceptováno s výhradami. V případě, že budou v průběhu akceptačního řízení zjištěny v předaném plnění (nebo jeho části) vady nebo nedodělky, a to v počtu 0 vad kategorie A a/nebo maximálně 5 vad kategorie B a/nebo maximálně 10 vad kategorie C, dohodnou se kupující a prodávající na termínu, do kterého prodávající tyto vady a nedodělky odstraní. Kupující do Akceptačního protokolu uvede seznam vad nebo nedodělků s termíny jejich odstranění. V Akceptačním protokolu se uvede, že předané plnění (nebo jeho část) bylo akceptováno s výhradami a obě strany Akceptační protokol potvrdí svým podpisem. Po odstranění všech vad a nedodělků podepíší obě smluvní strany nový Akceptační protokol s výsledkem „Akceptováno bez výhrad".

Neakceptováno. V případě, že budou v průběhu akceptačního řízení v předaném plnění stanoveny takové vady a nedodělky a to v počtu 1 a více vad kategorie A a/nebo 6 a více vad kategorie B a/nebo více než 10 vad kategorie C, není předané plnění (nebo jeho část) akceptováno. Obě strany se dohodnou na termínech nového předání a nového akceptačního řízení. Do Akceptačního protokolu se uvede, že předané plnění (nebo jeho část) nebylo akceptováno, dohodnuté termíny nového předání a akceptačního řízení a obě smluvní strany Akceptační protokol potvrdí svým podpisem.

6) V rámci kategorizace vad a stanovování výsledků akceptačního řízení je nepřípustné vady nebo nedodělky jakkoliv sdružovat nebo slučovat (např. 2 obdobné vady kategorie B nelze považovat za 1 vadu kategorie B apod.). Konečné rozhodnutí o kategorizaci vad předávaného plnění při akceptačním řízení přísluší kupujícímu.

7) Nedohodnou-li se smluvní strany jinak, maximální lhůta na odstranění vady kategorie A nepřesáhne 7 (slovy: sedm) kalendářních dnů od data podpisu Akceptačního protokolu a maximální lhůta na odstranění vad kategorie B a C nepřesáhne 5 (slovy: pět) pracovních dní od data podpisu Akceptačního protokolu se stavem „Akceptováno s výhradami". Odstranění vad je základní podmínkou pro zahájení předání/převzetí plnění jako celku. Lhůty na odstranění vad uvedené v tomto odstavci se vztahují pouze na vady a incidenty zjištěné před uvedením plnění do provozu.

8) K podpisu Akceptačního protokolu je oprávněn statutární orgán smluvní strany, dále oprávněná osoba smluvní strany, případně těmito osobami pověřená osoba, nebude-li vyplývat ze smlouvy nebo jiného závazného dokumentu jinak.

9) Akceptace školení proběhne na základě následující procedury.

   Po řádném ukončení jednotlivých školení bude sepsán protokol o uskutečnění příslušného školení, který bude obsahovat:

   a) označení, že se jedná o protokol o provedení školení na základě smlouvy;

   b) specifikaci předmětu školení;

   c) určení účastníků školení;

   d) datum uskutečnění školení a podpis oprávněné osoby za stranu kupujícího a za stranu prodávajícího;

   e) vizuální identitu projektů dle Pravidel pro provádění informačních a propagačních opatření.

Po řádném provedení uceleného souboru školení předpokládaného v rámci provedení dodávky sepíší strany Akceptační protokol potvrzující řádné provedení této části dodávky.

10) Bez ohledu na jiná ustanovení smlouvy se každá část plnění považuje za řádně provedenou po podpisu Akceptačního protokolu vztahujícího se k příslušné části plnění.

11) Plnění se považuje za řádně provedené předáním a převzetím všech jeho částí. Kupující podepíše prodávajícímu závěrečný (finální) Akceptační protokol, jestliže výsledky všech akceptačních procedur vyhověly stanoveným kritériím, celé plnění splňuje podmínky a vlastnosti stanovené smlouvou, je plně funkční a způsobilé pro použití ke smluvenému účelu, odpovídá sjednané funkční a technické specifikaci a parametrům uvedeným ve smlouvě a v zadávací dokumentaci předmětné veřejné zakázky a je bez jakýchkoliv nedodělků a vad. Závěrečné celkové předání/převzetí celého plnění je možné pouze na základě akceptačního řízení s výsledem „Akceptováno bez výhrad".

12) Smluvní strany se dohodly, že kupující je oprávněn pověřit oprávněnou osobu kupujícího provedením všech úkonů souvisejících s provedením akceptační procedury a předáním a převzetím plnění.

PŘÍLOHA Č. 4 KE KUPNÍ SMLOUVĚ

SPECIFIKACE LICENCÍ

Nemocnice Rudolfa a Stefanie Benešov, a.s.

safetica®

SPECIFIKACE LICENCÍ

Licence se poskytuje na dobu, sjednanou v kupní smlouvě, a pro ve smlouvě sjednaný počet stanic. Zákazník není oprávněn instalovat ani užívat Software na větším počtu stanic, než pro který mu byla poskytnuta licence. Uživatel není oprávněn používat hardwarové nebo softwarové prostředky, které by sdružovaly více stanic tak, aby obešel množstevní omezení licence pro sjednaný počet stanic (zákaz multiplexování).

Licencování nezávisí na serverových komponentách Safetica, pouze na počtu klientských stanic. V případě použití Safetica na terminálovém serveru je nutné pořídit licenci pro každého uživatele.

Specifikace a rozsah licence
700x Safetica DLP Perpetual

Ve věcech neupravených v této specifikace licencí a kupní smlouvě se užívání Software řídí Licenčními podmínkami Safetica, podrobně na odkaze:

https://cdn.safetica.com/web/safetica/files/licencni_podminky_Safetica_dokumentace_CZ_03_2018.pdf