



EVROPSKÁ UNIE  
Evropský fond pro regionální rozvoj  
Integrovaný regionální operační program



MINISTERSTVO  
PRO MÍSTNÍ  
ROZVOJ ČR



## SMLOUVA O DÍLO

(dále jen „smlouva“)

uzavřená ve smyslu ust. § 2586 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů, (dále jen „ObčZ“)

### Objednatel:

#### Statutární město Kladno

se sídlem: náměstí Starosty Pavla 44, 272 52 Kladno  
IČO: 00234516  
ID datové schránky: dyubpcm  
zastoupené: Ing. Danem Jiránkem, primátorem statutárního města

### Zhotovitel:

#### Síť, spol s r. o.

se sídlem: Pražákova 702/12, Mariánské Hory, 709 00 Ostrava  
IČO: 60779420  
DIČ: CZ60779420  
za níž jedná: XXXXXXXXXX  
zapsaná v Obchodním rejstříku vedeném Krajským soudem v Ostravě,  
spisová značka C 6504  
tel.: +420 596 624 458, e-mail: sales@sit.cz  
bankovní spojení: XXXXXXXXXX  
číslo účtu: Komerční banka, a. s.

dále společně jako „smluvní strany“

### I. Preambule

Objednatel je příjemcem dotace na projekt „Zajištění kybernetické bezpečnosti Statutárního města Kladna“ (dále jen „ZKB Kladno“), registrační číslo projektu CZ.06.3.05/0.0/0.0/15\_011/0006958. Projekt je spolufinancován z Integrovaného regionálního operačního programu (IROP). Tato smlouva je uzavírána na základě výsledku zadávacího řízení s názvem „Dodávka a implementace vybraných nástrojů kybernetické bezpečnosti statutárního města Kladno“ - Nástroje kybernetické bezpečnosti uveřejněném ve věstníku veřejných zakázek pod evidenčním číslem Z2019-023762.

### II. Předmět smlouvy

- 1) Předmětem smlouvy je závazek zhotovitele provést pro objednatele dílo spočívající v dodávkách a implementaci vybraných řešení v rozsahu dle zadávací dokumentace veřejné zakázky „Dodávka a implementace vybraných nástrojů kybernetické bezpečnosti statutárního města Kladno“ - Nástroje kybernetické bezpečnosti, nabídky zhotovitele a přílohy č. 1 této smlouvy. Dodávka bude zahrnovat zejména:



- Dodávku DLP (SW) vč. instalace a testování zahrnující potřebné licence potřebné pro použití v rámci rozsahu dodávky a podporu dodaného řešení v délce 60 měsíců.
  - Integraci dodaného díla se stávajícím aplikačním (SW, IS) vybavením zadavatele.
  - Integraci dodaného díla se stávajícím HW vybavením zadavatele.
  - Implementace dodaného SW do TC zadavatele.
  - Zaškolení obsluhy (min. 3 administrátorů) IS v délce 2 školících dnů (2 x po 8 hodinách) v rámci dodávky aplikačního vybavení (IS).
  - Záruční servis v délce trvání 60 měsíců.
- 2) Předmětem smlouvy je dále zajištění servisní podpory, provozu a rozvoje díla, včetně nákladů na rozvoj, provoz, servisní zásahy a havárie na dobu 10 let (6. až 15. rok), kdy náklady mohou činit maximálně 3.000.000,-Kč bez DPH za celou dobu 10 let a cena za 1 hodinu práce nesmí překročit 1.300,-Kč bez DPH. Rozvoj systému (materiálové položky) budou fakturovány dle cen uvedených v nabídce pro počáteční investice, které tvoří přílohu č. 3. V případě, že to nebude možné, budou fakturovány dle cen v místě a čase obvyklých.
- 3) Zhotovitel má právo cenu za 1 hodinu práce a za rozvoj systému (materiálové položky) valorizovat jednou ročně o oficiální míru inflace vyhlášenou Českým statistickým úřadem bez vyvolání cenového jednání. Své rozhodnutí o uplatnění inflační doložky oznámí zhotovitel objednateli písemně minimálně měsíc před uplatněním valorizace.
- 4) Zhotovitel se zavazuje provést na svůj náklad a na své nebezpečí všechna související plnění a práce potřebné k včasnému a řádnému provedení díla.
- 5) Součástí smlouvy je i převod neomezeného vlastnického práva k tomuto dílu na objednatele nebo práva k užití v případě SW licencí. Součástí závazku zhotovitele je rovněž doprava zboží objednateli do místa plnění, jeho instalace a zprovoznění podle pokynů objednatele, a dále provádění záručních oprav díla.
- 6) Objednatel se zavazuje dílo řádně a včas dodané zhotovitelem převzít a zaplatit za něj sjednanou kupní cenu způsobem a v termínu sjednaném touto smlouvou.
- 7) Práce nad rozsah díla dle této smlouvy (vícepráce), budou realizovány, jen pokud o ně bude po vzájemné dohodě písemným dodatkem k této smlouvě dílo rozšířeno.

### III. Doba a místo plnění

- 1) Zhotovitel se zavazuje, že dílo dodá objednateli nejpozději do tří měsíců od účinnosti smlouvy. Zhotoviteli bude umožněn přístup do místa plnění. V případě prodlení s řádným dodáním díla v termínu dle předchozí věty se zhotovitel zavazuje uhradit objednateli smluvní pokutu ve výši 0,05 % z ceny díla za každý i započatý den prodlení. Celková výše smluvní pokuty není omezena.
- 2) Objednatel si zároveň vyhrazuje právo termín ukončení plnění posunout z objektivních důvodů na straně objednatele (v souvislosti s termínem ukončení realizace úprav prostor pro serverovnu OV TI).
- 3) Provedením díla se rozumí úplné dodání a dokončení díla prostého podstatných vad bránících jeho funkcionalitě k účelu, k němuž má být využíváno a současně řádné protokolární předání díla objednateli.
- 4) Místem dodání plnění je dle této smlouvy sídlo objednatele, tedy Statutární město Kladno, náměstí Starosty Pavla 44, 272 52 Kladno a další dle zadávací dokumentace.

### IV. Podmínky provádění díla

- 1) Zhotovitel je povinen umožnit objednateli kontrolu provádění díla, popřípadě dalších osob pověřených objednatelům a poskytnout jim potřebnou součinnost a podmínky pro výkon jejich funkce.



- 2) Objednatel bude s ohledem na rozsah předmětu díla organizovat minimálně 1x měsíčně kontrolní dny (dále jen „KD“), kterých se zhotovitel zavazuje zúčastnit. Harmonogram jednotlivých KD bude plánovat objednatel v součinnosti s oprávněnou osobou zhotovitele.

#### V. Předání a převzetí díla

- 1) Po dokončení díla je zhotovitel povinen jej fyzicky předat objednateli v místě plnění a objednatel je povinen jej převzít, nebude-li vykazovat vady. K převzetí díla je zhotovitel povinen vyzvat objednatel nejméně 5 pracovních dnů předem, a to zasláním e-mailu na adresy osob oprávněných jednat za objednatele ve věcech technických.
- 2) Objednatel je oprávněn, nikoliv však povinen, dílo převzít s vadami a nedodělky, které samy o sobě ani ve spojení s jinými nebrání funkčnímu užívání díla, ani jeho užívání podstatným způsobem neomezují.
- 3) O předání a převzetí díla bude objednatel sepsán předávací protokol, ve kterém musí být výslovně uvedeno, zda objednatel dílo přebírá či nikoliv. Pokud objednatel dílo převezme s drobnými vadami či nedodělky nebránícími užívání, musí být tyto v předávacím protokolu uvedeny a musí být stanovena lhůta k jejich odstranění. Nedohodnou-li se strany na lhůtách pro odstranění vad, je zhotovitel povinen vady odstranit ve lhůtě do 15 dnů ode dne předání díla. V případě neodstranění vad zhotovitelem se použije ustanovení čl. III. odst. 1) smlouvy. V předávacím protokolu, event. jeho přílohách, musí být zejména uvedeno:
- označení díla, název a číslo projektu
  - označení objednatele a zhotovitele díla,
  - číslo a datum uzavření smlouvy o dílo,
  - evidenční údaje díla,
  - zahájení a dokončení prací na zhotovovaném díle,
  - prohlášení objednatele, zda dílo přejímá či nikoliv, a v případě nepřevzetí jeho důvody.
  - datum a místo sepsání zápisu,
  - jména a podpisy zástupců objednatele a zhotovitele,
  - seznam převzaté a odsouhlasené kompletní dokumentace (viz odst. 5, tohoto článku),
  - soupis vad a nedodělků nebránících užívání, pokud je dílo obsahuje, s termínem jejich odstranění,
  - 
  - datum ukončení záruky na dílo,
  - celková cena díla dle této smlouvy včetně výše plánované finanční podpory.
- 4) Dílo se považuje za předané okamžikem, kdy je jeho předání a převzetí potvrzeno oběma smluvními stranami podpisem předávacího protokolu. Za objednatele kontaktní osoba ve věcech technických, za zhotovitele zástupce společnosti - kontaktní osoba ve věcech technických.
- 5) Zhotovitel je povinen předat objednateli níže uvedené doklady a to **ve 3 vyhotoveních**:
- harmonogram prací dle skutečné realizace díla
  - dokumentace pro provoz zařízení, výrobků a jiné,
  - dokumentace pro údržbu zařízení, výrobků a jiné,
  - a případně další potřebné doklady, které budou během realizace dohodnuty mezi objednatel a zhotovitelem.

Náklady na pořízení všech těchto dokladů jsou zahrnuty v ceně díla.



## VI. Záruka za jakost díla a odpovědnost za vady

- 1) Zhotovitel poskytuje záruku za jakost díla podle této smlouvy v délce trvání 60 měsíců od dne předání a převzetí díla na základě předávacího protokolu potvrzeného oběma smluvními stranami a začíná běžet dnem předání a převzetí díla bez vad a nedodělků.
- 2) Zhotovitel po dobu záruky odpovídá za to, že jakost díla bude odpovídat této smlouvě a zejména všem částem předmětu díla uvedeným v čl. II. této smlouvy a příslušným normám, právním předpisům a směnicím platným v době provádění díla.
- 3) Smluvní strany si sjednávají nárok objednatele na bezplatné odstranění veškerých vad díla reklamovaných kdykoliv během záruční doby bez ohledu na dispoziční ustanovení zákona.
- 4) Objednatel je oprávněn reklamovat v záruční době vady předmětu díla u zhotovitele, a to písemnou formou. V reklamaci musí být popsána vada předmětu díla, určen nárok objednatele z vady předmětu díla, případně požadavek na způsob odstranění vad, a to včetně termínu pro odstranění vad zhotovitelem. Objednatel má právo volby způsobu odstranění důsledku vadného plnění. Za písemnou formu je považováno také nahlášení standardními prostředky technické podpory provozu, např. e-mailem nebo prostřednictvím helpdesku.
- 5) Součástí záruky je i poskytování podpory software v rozsahu:
  - poskytování aktuálních verzí dodaného software, tj. nabídka aktuálních verzí, upgrade a update dodaného software (SW maintenance),
  - legislativní servis, kdy aktuální verze dodaného software musí být zadavateli poskytnuta nejpozději k datu nabytí účinnosti nové právní úpravy za předpokladu vydání prováděcích předpisů k této úpravě nejpozději 60 dnů před nabytím účinnosti této nové právní úpravy (v opačném případě do 60 dnů od vydání prováděcích předpisů k příslušné právní úpravě).
- 6) Zhotovitel se zavazuje od okamžiku oznámení vady předmětu díla či jeho části zahájit odstraňování vady či jeho části, a to i tehdy, neuznává-li zhotovitel odpovědnost za vady či příčiny, které ji vyvolaly, a vady odstranit v technicky co nejkratší lhůtě, a současně zahájit reklamační řízení v místě provádění předmětu díla. O reklamačním řízení budou objednatelem požity písemné zápisy ve dvojnásobném vyhotovení, z nichž jeden stejnopis obdrží každá ze smluvních stran. Bude-li v reklamačním řízení vada uznána jako reklamační vada, bude odstranění vady předmětu díla či jeho části provedeno bezúplatně.
- 7) Záruka se nevztahuje na vady prokazatelně způsobené neodbornou manipulací nebo mechanickým poškozením objednatelem.

## VII. Servisní zásahy a sankce

- 1) Zhotovitel je povinen nastoupit v režimu 7 x 24 x 365 k odstranění reklamovaných vad díla a k servisním zásahům v následujících lhůtách od okamžiku doručení vyzvy objednatele:
  - **Time to response** – časový úsek **2 hodiny** od přijetí nahlášení požadavku na havarijní zásah Objednatelem do okamžiku potvrzení přijetí takového požadavku Zhotovitelem.
  - **Time to fix** – časový úsek **8 hodin** od přijetí nahlášení požadavku na havarijní zásah Objednatelem do zprovoznění služeb komponenty alternativním (dočasným) způsobem Zhotovitelem.
  - **Time to repair** – časový úsek **30 dní** od smluvními stranami odsouhlaseného technického řešení finálního způsobu opravy poruchy do okamžiku odstranění příčiny poruchy Zhotovitelem.

Rozhodující pro začátek doby pro odstranění poruchy bude čas písemného nahlášení Objednatelem na pracoviště technické podpory Zhotovitele.



- 2) Smluvní strany se mohou v odůvodněných případech dohodnout na prodloužení výše uvedených lhůt.
- 3) V případě, že zhotovitel nenastoupí k odstranění vady či neodstraní vadu ve shora uvedených lhůtách ani v dodatečné lhůtě, kterou mu k tomu objednatel stanoví, je objednatel oprávněn, a to bez ohledu na to, zda zhotovitel reklamaci či potřebnost servisního zásahu uznává či neuznává, pověřit odstraněním vady jinou právnickou nebo fyzickou osobou, a to za cenu obvyklou, a zhotovitel je povinen objednateli veškeré takto vzniklé náklady nahradit, přičemž objednateli nevzniká jakákoli ztráta záruky na dílo. V případě nedodržení lhůt, uvedených v čl. VII. bod 1), je výše pokuty následující:
  - Time to response - výše smluvní pokuty je 500,- Kč za každou započatou hodinu prodlení.
  - Time to fix - výše smluvní pokuty je 1.000,- Kč za každou započatou hodinu prodlení.
  - Time to repair - výše smluvní pokuty je 1.500,- Kč za každý započatý den prodlení.maximální výše pokuty může činit 5.000,-Kč za započatý den.
- 4) Záruka za jakost se u konkrétní vady nebo dodávky prodlužuje o dobu, po kterou bude trvat odstraňování vad zhotovitelem.
- 5) Dílo má vady, jestliže provedení díla neodpovídá požadavkům uvedeným ve smlouvě, příslušným právním předpisům, normám nebo jiné dokumentaci vztahující se k provedení díla, popřípadě pokud neumožní užívání, k němuž bylo určeno a zhotoveno.

### VIII. Cena a platební podmínky

- 1) Cena díla je stanovena na základě nabídkové ceny zhotovitele ze dne 22.1.2020 kalkulované v rámci zadávacího řízení na předmět plnění dle této smlouvy a její podrobný rozpis tvoří přílohu č. 2, která je nedílnou součástí této smlouvy.
- 2) Cena díla je blíže specifikována v příloze č. 2 této smlouvy. Cena díla dle čl. II odst. 1) smlouvy, rozdělená na cenu za počáteční investici a za provozní náklady za 60 měsíců (dobu udržitelnosti projektu), která činí celkovou částku ve výši 7 395 550 Kč bez DPH (slovy: sedm milionů tři sta devadesát pět tisíc pět set padesát korun českých). DPH ve výši 21% činí 1 553 066 Kč (slovy: jeden milion pět set padesát tři tisíc šedesát šest korun českých), cena celkem včetně DPH činí 8 948 616 Kč (slovy: osm milionů devět set čtyřicet osm tisíc šest set šestnáct korun českých). Cena započaté hodiny za servisní zásahy nad rámec záruky a havárie (60 měsíců) činí dle této smlouvy 1.250 Kč bez DPH a celkové servisní náklady nad rámec záruky a havárie za 60 měsíců mohou dle smlouvy činit max. 800.000 Kč bez DPH. Cena započaté hodiny za náklady na rozvoj, provoz, servisní zásahy a havárie na dobu 10 let (6. až 15. rok) činí dle této smlouvy 1.250 Kč bez DPH a celkové náklady za náklady na rozvoj, provoz, servisní zásahy a havárie na dobu 10 let (6. až 15. rok) mohou dle smlouvy činit max. 3.000.000 Kč bez DPH.
- 3) Cena díla zahrnuje základní servisní podporu na dodané dílo v délce trvání 60 měsíců od spuštění ostrého provozu díla.
- 4) Cena díla dále zahrnuje zejména dopravu, instalaci a implementaci a zprovoznění díla. Cena díla zahrnuje i náklady na správní poplatky, daně, cla, schvalovací řízení apod. (je-li relevantní), pojištění, přepravní náklady apod. Celková cena díla je stanovena dohodou smluvních stran a jako cena nejvýše přípustná.
- 5) Cena díla zahrnuje také veškeré náklady spojené s rozhraním (integrací), vzniklých na straně zhotovitele, popř. vyvolaných nutností obchodní spolupráce mezi zhotovitelem a dodavateli stávajících aplikací, na něž je požadována integrace (rozhraní). Požadavek objednatele je, aby zhotovitel uvedl a zahrnul do ceny plnění veškeré náklady spojené jak s vytvořením rozhraní, tak jeho udržováním v rámci záruční doby, zejména při změnách vyvolaných updatem aplikací zhotovitele a to jak v souvislosti se změnami legislativy, tak v souvislosti s inovacemi aplikací zhotovitele, a to vč. úprav vzniklých na straně zhotovitele, popř. vyvolaných nutností obchodní spolupráce mezi zhotovitelem a dodavateli stávajících aplikací, na něž je požadována integrace.
- 6) Změny předmětu díla a s tím související změny ceny díla, jejichž potřeba vznikne v důsledku okolností, které smluvní strany j ednající s náležitou péčí nemohly předvídat, budou řešeny v písemném dodatku ke smlouvě, který smluvní strany uzavřou za účelem provedení prací a dodávek nad rámec předmětu díla (dále jen „vícepráce“) či naopak neprovedení některých prací a dodávek,



kteřé byly součástí předmětu díla (dále jen „méněpráce“) či obojího současně (společně též „dodatečné práce“), pokud je jejich provedení nezbytné. To samé platí také v případě, kdy v průběhu realizace díla dojde k zjištění skutečností odlišných od dokumentace předané objednatelem, a tyto mají vliv na cenu díla.

- 7) Dodatek ke smlouvě může být uzavřen pouze na základě odsouhlaseného Změnového výkazu výměr objednatelem, konkrétně osobou oprávněnou jednat ve věcech technických dle čl. IX. odst. 10) této smlouvy.
- 8) Při sestavování Změnového výkazu výměr budou jednotlivé položky oceňovány následujícím způsobem:
  - a) Dodatečné dodávky a služby, jejichž položky jsou obsaženy v původním kalkulačním listu, budou oceněny podle jednotkové ceny těchto položek.
  - b) Dodatečné dodávky a služby, které nejsou obsaženy v původním kalkulačním listu, budou oceněny dle nabídky dodavatele.
- 9) Cenu díla je možné překročit pouze v souvislosti se změnou daňových předpisů upravujících výši DPH, přičemž v takovém případě bude ke kupní ceně připočteno DPH ve výši stanovené zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o dani z přidané hodnoty“).
- 10) Cena díla bude objednatelem uhrazena v korunách českých (CZK) na základě daňového dokladu (dále jen „faktura“) doručeného zhotoviteli.
- 11) Přílohou faktury musí být kopie akceptačního protokolu podepsaného osobami oprávněnými jednat za smluvní strany.
- 12) Cena servisní podpory bude objednatelem uhrazena vždy čtvrtletně, a to zpětně. Cena servisní podpory nezahrnuje cenu maintenance, která je zahrnuta v ceně za počáteční investici.
- 13) Faktura, musí obsahovat všechny náležitosti řádného daňového dokladu ve smyslu zákona o dani z přidané hodnoty. V případě, že faktura bude obsahovat věcné či formální nesprávnosti, popřípadě nebude obsahovat všechny zákonné náležitosti nebo přílohu dle předchozího odstavce, je objednatel oprávněn ji vrátit ve lhůtě splatnosti zpět zhotoviteli k doplnění či opravě, aniž se tak dostane do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněné či opravené faktury objednateli. Na faktuře bude uveden název a číslo projektu: Zajištění kybernetické bezpečnosti Statutárního města Kladna, CZ.06.3.05/0.0/0.0/15\_011/0006958.
- 14) Splatnost faktury se sjednává na 30 dnů ode dne doručení faktury objednateli.
- 15) Objednatel neposkytuje zhotoviteli zálohy na cenu díla.
- 16) V případě prodlení objednatele s úhradou splatné faktury je zhotovitel oprávněn uplatnit vůči objednateli pouze smluvní úrok z prodlení ve výši 0,05 % z dlužné částky za každý i jen započatý den prodlení s úhradou ceny díla.
- 17) Smluvní strany se výslovně dohodly, že objednatel je oprávněn započíst své i nesplacené pohledávky vzniklé na základě této smlouvy proti pohledávce zhotovitele na zaplacení ceny díla rovněž bez ohledu na její splatnost.
- 18) Zhotovitel se zavazuje, že v případě nabytí statutu „nespolehlivý plátc“ ve smyslu zákona o dani z přidané hodnoty, bude o této skutečnosti neprodleně objednatele informovat. Objednatel je poté oprávněn zaslat hodnotu plnění odpovídající dani z přidané hodnoty přímo na účet správce daně v režimu podle ust. §109a zákona o dani z přidané hodnoty.

## IX. Práva a povinnosti stran

- 1) Zhotovitel je povinen dodat objednateli úplné a funkční dílo dle této smlouvy a pokud je součástí dodávky i zboží, bude se jednat o nové nepoužité zboží v dohodnutém množství, jakosti a provedení, které je zhotovitel povinen předložit v souladu se specifikací technických a uživatelských standardů a objednatelem písemně odsouhlasenou dokumentací.



- 2) Zhotovitel je povinen v souladu s podmínkami této smlouvy řádně a včas dodat objednateli dílo dle této smlouvy, a to vč. implementace, provedení potřebné montáže, instalace a zprovoznění na místě plnění, přičemž za řádné dodání díla se považuje jeho převzetí objednatelem, a to na základě potvrzení této skutečnosti v protokolu o předání a převzetí dodávky díla. Předávací protokol může být podepsán nejdříve v okamžiku, kdy bude beze zbytku realizována dodávka díla zhotovitelem včetně dodání na místo určené objednatelem, instalace, implementace a zprovoznění díla s tím, že zhotovitel na své náklady zajistí odvoz a likvidaci obalů a dalších použitých materiálů a úklid prostor dotčených realizací dodávky zboží.
- 3) Zhotovitel je povinen spolu s dílem dodat objednateli kompletní dokumentaci nezbytnou k užívání zboží, a to zejména záruční listy a návody v českém jazyce a další dokumentaci vyplývající z platné legislativy, zejm. zákona č. 365/2000 Sb. o informačních systémech veřejné správy, ve znění pozdějších předpisů, přičemž je současně povinen provést proškolení obsluhy díla a potřebné revize.
- 4) Objednatel nabývá vlastnického práva k dílu a/nebo právo k užití SW licencí dnem řádného předání a převzetí díla od zhotovitele na základě podpisu předávacího protokolu oběma smluvními stranami. Stejným okamžikem přechází na objednatele také odpovědnost za nebezpečí škody na předmětu plnění dle této smlouvy.
- 5) Zhotovitel je povinen neprodleně písemně vyrozumět objednatele o případném ohrožení doby plnění a o všech skutečnostech, které mohou řádné a včasné plnění předmětu této smlouvy znemožnit, a to nejpozději do 3 dnů ode dne, kdy se zhotovitel dozví o takové skutečnosti.
- 6) Zhotovitel není oprávněn postoupit jakákoliv práva anebo povinnosti vyplývající z této smlouvy na třetí osoby bez předchozího písemného souhlasu objednatele.
- 7) Smluvní strany sjednávají, že zhotovitel není oprávněn jakékoliv jeho pohledávky za objednatelem, které vzniknou na základě této smlouvy, započítat vůči pohledávkám objednatele za zhotovitelem jednostranným právním jednáním.
- 8) Zhotovitel odpovídá objednateli za škodu způsobenou porušením povinnosti podle této smlouvy nebo povinnosti stanovené obecně závazným platným právním předpisem.
- 9) Smluvní strany se dohodly a zhotovitel určil, že osobou oprávněnou k jednání za zhotovitele v technických věcech, které se týkají této smlouvy a její realizace, je/Jsou:  
Jméno a příjmení: Tomáš Méheš  
e-mail: [tomas.mehes@sit.cz](mailto:tomas.mehes@sit.cz)  
tel.: +420 [REDACTED]
- 10) Smluvní strany se dohodly a objednatel určil, že osobou oprávněnou k jednání za objednatele v technických věcech, které se týkají této smlouvy a její realizace, je:  
Jméno a příjmení: Petr Jorg, MBA  
e-mail: [petr.jorg@mestokladno.cz](mailto:petr.jorg@mestokladno.cz)  
tel.: +420 312 604 445  
  
Jméno a příjmení: Petr Dusbábek, DiS.  
e-mail: [petr.dusbabek@mestokladno.cz](mailto:petr.dusbabek@mestokladno.cz)  
tel.: +420 312 604 800
- 11) Veškerá korespondence, pokyny, oznámení, žádosti, záznamy a jiné dokumenty vzniklé na základě této smlouvy mezi smluvními stranami nebo v souvislosti s ní budou vyhotoveny v písemné formě v českém jazyce a doručují se buď osobně, doporučenou poštou nebo prostřednictvím datové schránky, na adresu sídla, či ID datové schránky objednatele, uvedené v záhlaví této smlouvy. Smluvní strany se v případě doručování zásilek formou doporučených dopisů dohodly tak, že zásilka je považována za doručenu 3. pracovní den bezprostředně následující po dni jejího odeslání prostřednictvím držitele poštovní licence na adresu příslušné smluvní strany dle záhlaví této smlouvy.



- 12) Zhotovitel je povinen ve lhůtě do 10 pracovních dnů ode dne nabytí účinnosti této smlouvy uzavřít pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti zhotovitele za škodu způsobenou zhotovitelem do výše limitu pojistného plnění v částce minimálně 5 000 000,- Kč z jedné pojistné události ročně. Zhotovitel se zavazuje na žádost objednatele bezodkladně, nejpozději však ve lhůtě do 5 pracovních dnů od doručení písemné výzvy objednatele, předložit objednateli pojistný certifikát prokazující existenci a účinnost této pojistné smlouvy. Zhotovitel se zavazuje, že pojistná smlouva dle věty první tohoto článku zůstane v účinnosti v tomto rozsahu po celou dobu trvání záruky. Za porušení povinnosti dle tohoto odstavce zaplatí zhotovitel objednateli smluvní pokutu ve výši 5.000,-Kč bez DPH za každý, byť jen započatý den, v němž bude zhotovitel v prodlení.
- 13) Zhotovitel se zavazuje označovat veškeré vydané faktury číslem projektu uvedeném v Preambuli této smlouvy.
- 14) Zhotovitel je povinen minimálně do roku 2029 poskytovat požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.
- 15) Zhotovitel je povinen uchovávat veškerou dokumentaci související s realizací projektu včetně faktur minimálně do konce roku 2029. Pokud je v příslušných českých právních předpisech stanovena lhůta delší, musí ji zhotovitel použít.

#### **X. Platnost a účinnost smlouvy**

- 1) Tato smlouva nabývá platnosti dnem podpisu poslední ze smluvních stran a účinnosti okamžikem jejího uveřejnění v registru smluv. Smluvní strany berou na vědomí, že tato smlouva vyžaduje uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a registru smluv, ve znění pozdějších předpisů a s tímto uveřejněním souhlasí. Zaslání smlouvy do registru smluv se objednatel zavazuje zajistit neprodleně po podpisu smlouvy.
- 2) Zhotovitel bude pro Objednatele zajišťovat plnění předmětu smlouvy v rozsahu rozvoje, provozu, servisních zásahů a řešení havárií po dobu 10 let (6. až 15. rok), po ukončení doby udržitelnosti projektu (60 měsíců) dle bodu 2), článku VIII., nebo do vyčerpání celkového finančního limitu 3.000.000,-Kč bez DPH podle toho, která skutečnost nastane dříve. Ke dni ukončení smlouvy musí být vypořádány všechny platby.
- 3) Smluvní strany berou na vědomí, že smlouva bude zveřejněna v registru smluv v souladu se zákonem č. 340/2015 Sb., o registru smluv, v platném znění. Zveřejnění provede odpovědný zaměstnanec objednatele ve lhůtě 15 dnů ode dne podpisu smlouvy poslední smluvní stranou. Do 3 dnů pak protistranu informuje o splnění této povinnosti a o případných změnách a opravách provedených v registru smluv.
- 4) Odstoupit od smlouvy lze pouze z důvodů stanovených v této smlouvě nebo ObčZ.
- 5) Od této smlouvy může smluvní strana dotčená porušením povinnosti jednostranně odstoupit pro podstatné porušení této smlouvy druhou smluvní stranou, přičemž za podstatné porušení této smlouvy se považuje:
  - a) je-li objednatel v prodlení se zaplacením ceny díla podle této smlouvy po dobu delší než 60 dní po dni splatnosti příslušné faktury, ačkoliv byl na své prodlení písemně upozorněn a přes toto písemné upozornění objednatel nápravu neprovedl ve lhůtě do 30 dnů od doručení písemného upozornění;
  - b) jestliže zhotovitel dodá dílo, které nebude mít vlastnosti deklarované zhotovitelem v této smlouvě, resp. v nabídce zadávacího řízení, na jehož základě byla tato smlouva uzavřena;
  - c) jestliže zhotovitel dodá dílo, které je zatíženo právy třetích osob s výjimkou SW licencí.





- 6) Objednatel je dále oprávněn odstoupit bez jakýchkoliv sankcí od této smlouvy v případě, že mu nebude zcela nebo částečně udělena finanční dotace k pořízení předmětu plnění, nebo mu bude dotace odejmuta.
- 7) Odstoupením od této smlouvy zanikají všechny závazky smluvních stran z této smlouvy. V případě odstoupení od této smlouvy nezanikají nároky smluvních stran na náhradu škody a zaplacení smluvních pokut sjednaných pro případ porušení smluvních povinností vzniklé před skončením účinnosti této smlouvy, a ty závazky smluvních stran, které podle smlouvy nebo vzhledem ke své povaze mají trvat i nadále, nebo u kterých tak stanoví ObčZ.

## XI. Ochrana informací

- 1) Zhotovitel se zavazuje, že zachová jako citlivé informace a zprávy týkající se vnitřních záležitostí smluvních stran a předmětu plnění smlouvy, pokud by jejich zveřejnění mohlo poškodit druhou stranu. Povinnost poskytovat informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, není tímto ustanovením dotčena.
- 2) Smluvní strany budou považovat za citlivé informace a) jako citlivé označené, b) informace, u kterých se z povahy věci dá předpokládat, že se jedná o informace podléhající závazku mlčenlivosti nebo informace o objednateli, které by mohly z povahy věci být považovány za citlivé a které se dozvědí v souvislosti s plněním této smlouvy.
- 3) Smluvní strany se zavazují, že neuvolní třetí osobě informace druhé strany bez jejího souhlasu, a to v jakékoliv formě, a že podniknou všechny nezbytné kroky k zabezpečení těchto informací. Závazek mlčenlivosti a ochrany citlivých informací zůstává v platnosti po dobu 5 let po ukončení smlouvy.
- 4) Zhotovitel je povinen zabezpečit veškeré podklady, mající charakter citlivé informace poskytnuté mu objednatel, proti odcizení nebo jinému zneužití.
- 5) Zhotovitel je povinen svého případného poddodavatele zavázat povinností mlčenlivosti a respektováním práv objednatele nejméně ve stejném rozsahu, v jakém je v závazkovém vztahu zavázán sám.
- 6) V souvislosti s důvěrností informací bere zhotovitel na vědomí, že je zákonnou povinností objednatele uveřejnit celé znění této smlouvy včetně všech jejích případných dodatků a seznamu poddodavatelů v souladu se zákonem. Splnění této, jakož i dalších zákonných povinností objednatele, není porušením důvěrnosti informací.
- 7) Povinnost zachovávat mlčenlivost se nevztahuje na informace:
  - a) které jsou nebo se stanou všeobecně a veřejně přístupnými jinak, než porušením ustanovení tohoto odst. ze strany zhotovitele,
  - b) které jsou zhotoviteli známy a byly mu volně k dispozici ještě před přijetím těchto informací od objednatele,
  - c) které budou následně zhotoviteli sděleny bez závazku mlčenlivosti třetí stranou, jež rovněž není ve vztahu k nim nijak vázána,
  - d) jejichž sdělení se vyžaduje ze zákona.
- 8) Za prokázané porušení ustanovení v tomto čl. má druhá smluvní strana právo požadovat náhradu takto vzniklé škody.
- 9) V případě porušení povinností uložených smluvním stranám tímto odst. má druhá smluvní strana právo účtovat smluvní pokutu ve výši 100.000 Kč za každý případ porušení.

## XII. Závěrečná ustanovení

- 1) Uhrazením smluvních pokut dle této smlouvy není dotčen nárok na náhradu škody. Pro případ, že by byla smluvní pokuta soudem snížena, dohodly se zároveň smluvní strany, že zůstává zachováno



právo na náhradu škody ve výši, v jaké škoda převyšuje částku určenou soudem jako přiměřenou. Smluvní pokuty dle této smlouvy lze požadovat kumulativně, a to bez omezení. Úhradou smluvní pokuty zhotovitelem není dotčena další existence povinnosti smluvní pokutou zajištěné. Smluvní pokuta dle této smlouvy je splatná do 15 kalendářních dnů ode dne doručení písemného uplatnění práva na smluvní pokutu, a to na účet písemně určený objednatelem. Smluvní pokutu je objednatel oprávněn započíst oproti splatným pohledávkám zhotovitele.

- 2) Vztahy mezi smluvními stranami se řídí českým právním řádem. Ve věcech smlouvou výslovně neupravených se právní vztahy z ní vznikající a vyplývající řídí příslušnými ustanoveními ObčZ a ostatními obecně závaznými právními předpisy. Rozhodčí řízení je vyloučeno.
- 3) Nastanou-li u některé ze smluvních stran skutečnosti bránící řádnému plnění této smlouvy, je povinna to ihned bez zbytečného odkladu písemně oznámit druhé smluvní straně a vyvolat jednání objednatele a zhotovitele.
- 4) Vztahuje-li se důvod neplatnosti jen na některé ustanovení smlouvy, je neplatným pouze toto ustanovení, pokud z jeho povahy, obsahu anebo z okolností, za nichž bylo sjednáno, nevyplývá, že jej nelze oddělit od ostatního obsahu smlouvy. Smluvní strany se zavazují, že bezodkladně nahradí neplatné ustanovení této smlouvy jiným platným ustanovením svým obsahem podobným neplatnému ustanovení.
- 5) Smlouva je vyhotovena v jednom elektronickém originálu.
- 6) Zhotovitel potvrzuje, že poskytnuté osobní údaje uvedené v této Smlouvě jsou přesné a že se jedná o dobrovolné poskytnutí osobních údajů. objednatel je ve smyslu *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)* a zákona č. 110/2019 Sb. o zpracování osobních údajů, správcem osobních údajů subjektů údajů a že zpracovává a shromažďuje osobní údaje zhotovitele za účelem realizace této smlouvy. Objednatel se zavazuje zpracovávat osobní údaje zhotovitele pouze k účelu danému touto smlouvou, bez využití jiného zpracovatele údajů. Zhotovitel prohlašuje, že si je vědom všech svých zákonných práv v souvislosti s poskytnutím svých osobních údajů k účelu danému touto smlouvou. Podrobné informace o ochraně osobních údajů jsou uvedeny na oficiálních webových stránkách [www.mestokladno.cz](http://www.mestokladno.cz) v sekci Ochrana osobních údajů.
- 7) Nedílnou součástí této smlouvy jsou následující přílohy:
  - a) Příloha č. 1 – Specifikace technického řešení
  - b) Příloha č. 2 – Položkový rozpočet
  - c) Příloha č. 3 – Podrobný nabídkový rozpočet (z nabídky ve veřejné zakázce)
  - d) Příloha č.4 - Závazný harmonogram plnění

V Kladně dne \_\_\_\_\_

V ..... dne .....

Za Objednatele:


Za Zhotovitele:

*podepsáno elektronicky*

Ing. Dan Jiránek

primátor

Statutární město Kladno

 9.  
:09:12

Ing. Alena Sandriová

prokurista

SÍŤ, spol. s r. o.



## Příloha č. 1 zadávací dokumentace ve veřejné zakázce

# Technická specifikace předmětu zakázky (Technický list)



### Oblast: Nástroje kybernetické bezpečnosti (část 2 VZ)

**Cíl:** Žadatel identifikoval slabé místo v lokálním řízení přístupových práv. Předmětem opatření je pořízení nástrojů pro řízení přístupových oprávnění, jedná se o správu privilegovaných účtů se zabezpečeným úložištěm hesel a správou přístupů k těmto účtům včetně zaznamenávání aktivit privilegovaných účtů, včetně nahrávek obrazovek a stisků kláves a celých session s možností vyhledávání pomocí klíčových slov. Další součástí bude také disaster recovery pro umístění řešení do záložní lokality. Implementace bude obsahovat integraci na systémy Linux a Windows servery včetně přístupu na centrální prvky a vzdálený přístup na servery pomocí např. iDRAC. V neposlední řadě bude cílem předcházení ztráty nebo poškození dat u kritických operací prováděných pod privilegovanými účty pomocí nástroje DLP (Data Loss Prevention).

### **Opatření k realizaci:**

Žadatel pořídí a zavede **centrální správu privilegovaných účtů** se zabezpečeným úložištěm hesel a správou přístupů k těmto účtům a zaznamenávání aktivit až 105 privilegovaných účtů, včetně nahrávek obrazovek a stisků kláves a celých session s možností vyhledávání pomocí klíčových slov v prostředí Zadavatele. Návrh řešení bude zohledňovat také disaster recovery pro umístění řešení do záložní lokality Zadavatele.

### Požadavky na funkčnost:

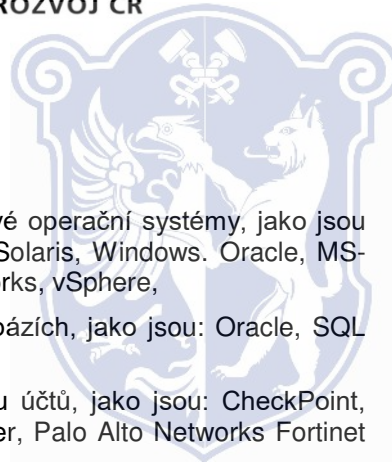
Dodavatel v rámci dodávky provede nejprve analýzu nezbytnou pro instalaci a konfiguraci komponent PIM řešení, Na základě požadavků na PIM řešení Dodavatel připraví návrh testovacích scénářů, pokrývajících testování všech funkčních rysů implementovaného řešení, včetně testování vybraných výkonových parametrů a výpadků jednotlivých komponent. Dále Dodavatel připraví návrh integrace PIM řešení do provozního a bezpečnostního monitoring systému Objednatele.

### Architektura:

- Systém je nabízen ve formě uzavřené fyzické platformy nebo uzavřené virtuální platformy připravené k implementaci v infrastruktuře klienta. Uzavřenou platformou rozumíme specializované řešení, v němž je nainstalován veškerý software (operační systém, databáze, aplikace) a implementuje funkcionalitu systému PAM.
- Systém bude postaven v koncepci architektury s vysokou dostupností HA (min. active-passive), včetně instalace systému do dvou nezávislých datových center (DC).
- Systém spravuje účty na cílových systémech v modelu bez agentů.
- Uživatelské rozhraní PAM je přístupné prostřednictvím webového prohlížeče.

### Ověřování, autorizace a oddělení práv:

- Systém umožňuje integraci uživatelských účtů PAM s mechanismy ověřování služby Microsoft Active Directory.
- Systém umožňuje použití dvoufaktorového ověřování (RADIUS).
- Systém umožňuje rozdělení rolí: Žadatel (provozovatel nebo správce v cílovém systému, musí žádat o přístup k sessions a heslům), Správce (řídící systém PAM), Auditor (oprávněného ke sledování a zobrazení relací s protokoly), Schvalovatel (schvalování žádostí o přístup k relacím a heslům).
- Systém umožňuje omezit uživatelský přístup (pro role Žadatel, Auditor, Schvalovatel) pouze na určené účty cílového systému.



#### Účty cílových systémů:

- Systém má podporu pro správu privilegovaných účtů na cílové operační systémy, jako jsou systémy AIX, IBM AS400, HP-UX, Unix, Linux, Mac OS X, Solaris, Windows, Oracle, MS-SQL, Cisco, Fortinet, Juniper, Checkpoint, F5, Palo Alto Networks, vSphere,
- Systém má podporu pro správu privilegovaných účtů v databázích, jako jsou: Oracle, SQL Server, MySQL, Sybase, Teradata.
- Systém má podporu pro privilegovaných zařízení pro správu účtů, jako jsou: CheckPoint, Cisco, Dell iDRAC, BIG-IP (F5), HP iLO, HP Comwar, Juniper, Palo Alto Networks Fortinet SonicWALL.
- Systém má podporu pro správu privilegovaných účtů v cloudových platformech a sociální platformy: Amazon AWS, Azure, Office 365, Google, GoGrid, Rackspace, Facebook, Twitter, Instagram, LinkedIn, Pinterest Xing.
- Systém umožňuje "vkládání" přístupových oprávnění na webové portály (pomocí serveru terminálových služeb) pomocí editovatelných skriptů.
- Systém umožňuje vkládání přístupových oprávnění do aplikace (pomocí serveru Terminálové služby) pomocí upravitelných skriptů.

#### Správa hesel (bezpečné heslo, vytváření a změna hesel na účtu):

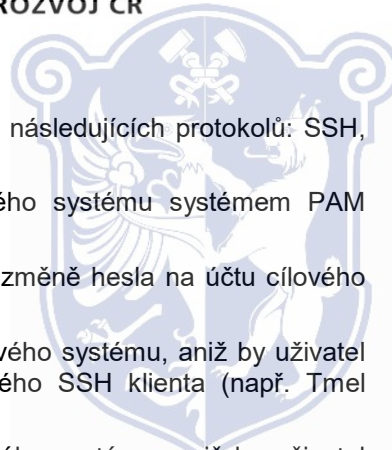
- Systém umožňuje definovat pravidla složitosti hesel.
- Pravidla složitosti hesel umožňují definovat požadavky na: délku hesla, znaky v hesle (malé a velké písmena, čísla, speciální znaky), možnost opětovného použití stejného hesla.
- Systém automaticky generuje heslo cílových systémových účtů pseudonáhodným způsobem v souladu s definovanými pravidly složitosti hesla.
- Systém vytváří jedinečná hesla pro cílový systémový účet.
- Systém umožňuje ruční změnu (inicializováno správcem) hesla na zadaném cílovém systémovém účtu.
- Systém umožňuje definování pravidel frekvence pro změnu hesla v cílových systémových účtech.
- Systém poskytuje automatickou změnu hesla v určených účtech cílových systémů v souladu s definovanou politikou frekvence změn hesla.
- Systém zajišťuje ověření shody hesla na účtu cílového systému s heslem uloženým v systému PAM.
- Mechanismus automatické změny hesla vám umožňuje změnit heslo v PAM. V případě neúspěšné propagace změny hesla z PAM na dotčené systémy, umí PAM zastoupit původní heslo v systému novým heslem již evidovaným v PAM do doby úspěšné propagace.
- Systém umožňuje prohlížení předchozích verzí hesel pro cílové systémy.

#### Správa klíčů:

- Systém umožňuje definovat pravidla pro typ klíče, délku klíče, passphrase.
- Systém umožňuje automatické generování klíčů v souladu s definovanými pravidly.
- Systém umožňuje definování pravidel frekvence pro změnu klíčů v cílových systémech.

#### Řízení relací:

- Systém umožňuje transparentní vytvoření relace k cílovému systému, aniž by uživatel musel zadat heslo pro privilegovaný účet pro Windows, Unix a Linux.



- Systém poskytuje shrnutí relací do cílového systému pomocí následujících protokolů: SSH, RDP.
- Systém zajišťuje zablokování a přerušení relace do cílového systému systémem PAM autorizovaným operátorem (auditorem).
- Systém poskytuje funkci "jednorázového" hesla spočívající v změně hesla na účtu cílového systému po ukončení relace k tomuto systému.
- Systém zajišťuje transparentní vytvoření SSH spojení do cílového systému, aniž by uživatel musel zadávat heslo privilegovaného účtu pomocí libovolného SSH klienta (např. Tmel MobaXterm).
- Systém poskytuje transparentní seznam relací RDP do cílového systému, aniž by uživatel musel zadat heslo pro privilegovaný účet pomocí libovolného klienta RDP.
- Systém umožňuje nastavit spravované připojení RDP / SSH pomocí libovolného klienta bez nutnosti přihlašování k webovskému portálu PAM.

#### Sledování a nahrávání:

- Systém poskytuje monitorování (náhled) relací sestavených systémem PAM do cílových systémů. Tato funkce je k dispozici pouze oprávněným uživatelům systému PAM.
- Systém umožňuje zaznamenávat přístupová oprávnění systému PAM do cílových systémů.
- Systém zajišťuje přehrávání relací zaznamenaných systémem PAM. Tato funkce je k dispozici pouze oprávněným uživatelům systému PAM.
- Systém zajišťuje registraci vydaných příkazů a provozních výsledků příkazů pro relace sestavené systémem PAM pomocí protokolu SSH na cílové systémy. Metoda registrace umožňuje textové vyhledávání.
- Systém zajišťuje registraci aktivity v relaci RDP, přičemž se vezmou v úvahu zadané řetězce, kliknutí myší, jména otevřených oken. Metoda registrace umožňuje textové vyhledávání.

#### Správa uživatelů a skupin:

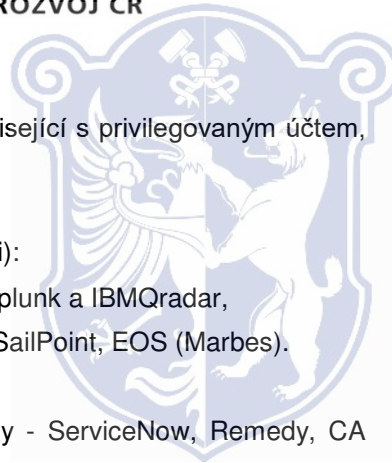
- Systém umožňuje řízení přístupu uživatelů systému PAM k heslům a/nebo cílovým relacím systémových účtů.
- Systém umožňuje přiřazení uživatelů systému PAM do skupin za účelem oddělení práv a zjednodušení procesu udělování práv.

#### Žádost o přístup a přístup k heslům, relacím:

- Systém umožňuje požadovat přístup k heslu a/nebo relaci, zatímco schvalovací schéma obsahuje následující modely: automatické přijetí, jednorázová akceptace schváleným operátorem, jednorázová akceptace více operátory.
- Systém vám umožňuje odeslat e-mailové upozornění uživateli, který požaduje přístup k heslu a/nebo relaci po dokončení procesu schvalování.
- Systém umožňuje určit typ přístupu, který může určitý uživatel získat (heslo účtu, nastavení relace RDP / SSH).

#### Audit a reportování:

- Systém poskytuje automatické reporty a zprávy "na požádání".
- Systém zajišťuje omezení přístupu k reportům pro danou skupinu administrátorů a/nebo uživatelů.
- Systém zajišťuje registraci a hlášení procesu vyžádání přístupu k heslu a/nebo relaci.



- Systém zajišťuje registraci a oznamování každé činnosti související s privilegovaným účtem, zejména změnou hesla na účtu a stažením hesla.

Integrace s jinými systémy (úplný rozsah integrace popsány v dokumentaci):

- Systém má integraci (vestavěný konektor) se systémy SIEM-Splunk a IBMQradar,
- Systém má integraci (vestavěný konektor) se systémy, IDM – SailPoint, EOS (Marbes).
- Systém má integraci na Logmanager ELISA
- Systém je integrován (integrovaný konektor) s ITSM systémy - ServiceNow, Remedy, CA Service Desk Manager, Jira.
- Systém umožňuje použití rozhraní API umožňující implementaci základních funkcí PAM.
- Systém umožňuje odesílání událostí systému (syslog).
- Tvorba dokumentace:
  - Instalační dokumentace
    1. Popis architektury
    2. Komunikační matice komponent
    3. Instalované verze
    4. Licence
    5. Instalační postup
  - Implementační dokumentace
    1. Popis nastavení komponent PIM řešení
    2. Popis způsobu integrace s AD
    3. Popis konfigurace zálohování PIM řešení
  - Uživatelská příručka
    1. Popis uživatelského rozhraní PIM řešení z pohledu uživatele
    2. Popis uživatelských postupů při práci PIM řešení
  - Administrátorská příručka
    1. Popis uživatelského rozhraní PIM řešení z pohledu administrátora
    2. Popis základních úkonů nutných pro údržbu PIM řešení a standardní profylaktické testy
  - Zajištění kontinuity provozu
    1. Popis postupu obnovy ze zálohy
    2. Doporučení pro archivaci (nahrané uživatelské relace a související data)
    3. Popis postupu v případě havárie jednotlivých komponent včetně postupu obnovy do provozního stavu
    4. Popis postupu nouzového přístupu k systémům Města v případě nedostupnosti/omezené funkčnosti PIM řešení
- Školení
  - Dodavatel zajistí proškolení min. 3 osob objednavatele v rozsahu 2 školících dnů (2 x po 8 hodinách) na úrovni administrace

Rozsah:

Cílem je do Session Recordingu a Password Managementu postupně zahrnout celkem 100 virtuálních/fyzických OS Windows a Linux. Počet uživatelů 105 kdy se jedná o 15 interních správců a 90 účtů externích správců.

Pro pokrytí řízení přístupových práv nástrojem může být, jako podpůrné opatření, použito řešení DLP, které bude zajišťovat předcházení ztráty nebo poškození dat u kritických operací prováděných pod privilegovanými účty.



## Definování podpůrného opatření DLP (Data Loss Prevention)

Cílem je zajištění přehledu činnosti uživatele se soubory a adresáři a v případě vzniku bezpečnostní události operaci zaznamenat a varovat správce. Dále bude řešeno:

- Instalace klientů (koncová zařízení uživatelů, terminálové servery)
- Konfigurace a nastavení politik
- Odzkoušení funkčnosti
- Propojení
- Tvorba dokumentace

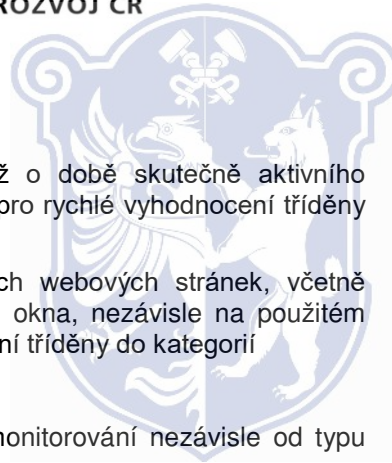
V současné době Město má celkem 445 aktivních účtů z toho je 340 uživatelů s oprávněním běžného uživatele a 85 externích uživatelů (správců inf. systémů) a 20 účtů interních správců systémů.

**DLP** musí minimálně splňovat tyto požadavky:

### 1. Všeobecné požadavky

- a. Integrace s Active Directory
- b. Podpora databázového SQL serveru 2008 R2 a novější
- c. Podpora OS Windows 7 a vyšší
- d. Podpora OS Windows Server 2008 R2 a vyšší
- e. Podpora terminálového prostředí (RDP, Citrix)
- f. Centrální administrativní konzole s přizpůsobením dle oprávnění
  - i. Možnost auditu přístupu k výsledkům a nastavením produktu, řízení přístupových oprávnění k administraci
- g. Skrytý režim vč. skrytí procesu a složek a to i vzhledem k lokálnímu nebo doménovému administrátorovi přítomnému na koncové stanici
- h. Ochrana proti obejití systému
  - i. Ochrana systému proti obejití musí být aktivní pro uživatele, lokálního i doménového administrátora
  - ii. Nemožnost zastavit procesy, v případě zvýšených práv automatické obnovení nebo jiná ochrana
  - iii. Nemožnost odinstalace bez explicitní autorizace
  - iv. Nemožnost změny registru, zásahu do komponent systému, knihoven DLL
  - v. Nemožnost měnit nastavení z koncové stanice
  - vi. Musí existovat řešení pro ochranu v nouzovém režimu (safe mode)
- i. Funkčnost musí přetrvávat také v tzv. offline režimu mimo připojení do firemní sítě nebo na internet
- j. Možnost práce s historickými daty
- k. Řešení musí podporovat nebo přímo poskytovat zálohování vlastních komponent, zejména záznamů a konfigurace
- l. Generování automatických emailových zpráv v případě vzniku incidentu, lze přizpůsobit prahy citlivosti i specifikaci incidentu
- m. Generování automatických reportů do emailu, tyto lze plně přizpůsobit (jaké informace, za jaké uživatele, jak často a komu budou přicházet)
- n. Možnost posílání záznamů do SIEM systému
- o. MDM řešení pro Android, iOS a Windows Phone

### 2. Požadavky na bezpečnostní audit



- a. Obecné požadavky
    - i. podrobné informace o době spuštění a rovněž o době skutečně aktivního využívání konkrétních aplikací, tyto jsou zároveň pro rychlé vyhodnocení tříděny do kategorií
    - ii. 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
    - iii. Možnost exportu záznamů do XLS, PDF
  - b. Instant Messenger aplikace, webový email – možnost monitorování nezávisle od typu aplikace nebo služby
  - c. E-mail:
    - i. Podpora protokolů POP3, IMAP, MAPI / Exchange vč. šifrování SSL
    - ii. Podpora emailového klienta MS Outlook, Thunderbird, Icwarp – řešení je schopné monitorovat e-mailové aplikace, nezávisle na typu aplikace
  - d. Pohyb dat:
    - i. 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
    - ii. Lokální operace se soubory – kopírování, přesun, stažení z webu, FTP, mazání, vytváření, otevírání včetně identifikace zdrojové a cílové lokality – cesta, typ zařízení, jednoznačný identifikátor
    - iii. Logování vytištěných dat
    - iv. Použití kopírování do schránky a snímání obrazovky
  - e. Aktivita na stanici:
    - i. Log zapnutí/vypnutí PC
    - ii. Log přihlášení/odhlášení uživatele
    - iii. Log spánku/vzbuzení PC
  - f. Síťová aktivita:
    - i. Objem stažených a zaslaných dat
3. Ochrana dat
- a. Obecně:
    - i. Nezávislost na aplikaci, protokolu vč. šifrovaného spojení
    - ii. Řešení je odolné vůči obejití ochrany na souborovém systému při použití odkazů na jiné složky včetně symbolických odkazů a podobných technologií
  - b. Šifrování:
    - i. Šifrování celých disků (Full Disk Encryption) i pro systémové disky
    - ii. Šifrování souborů
    - iii. Virtuální šifrované disky
    - iv. Vynucení šifrování v předem definovaných akcích (zasílání dat na neautorizovaná úložiště)
  - c. Data Loss Prevention
    - i. 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

- ii. Možnost monitorovacího, upozorňovacího i zakazovacího režimu
  - iii. Možnost navázání politik na konkrétní aplikace – definice zdrojů (konkrétní data, přístup k externím zařízením, síti), které aplikace může využít pro svůj běh
- d. Device Control
- i. Globální omezení na USB, firewire, mobilní telefony, paměťové karty, LPT, COM, Bluetooth, CD, DVD, Blue-ray
  - ii. Možnost read-only módu
  - iii. Auditní záznam veškerých externích zařízení připojovaných do systému vč. monitoru, klávesnic a myši



## 6 Podrobná specifikace nabízených technologií a jejich implementace

Uchazeč, společnost SÍŤ, spol. s r.o., nabízí pro plnění veřejné zakázky pro správu privilegovaných účtů (PAM) řešení od společnosti BeyondTrust. Pro zajištění DLP nabízí uchazeč řešení od společnosti Safetica Technologies.

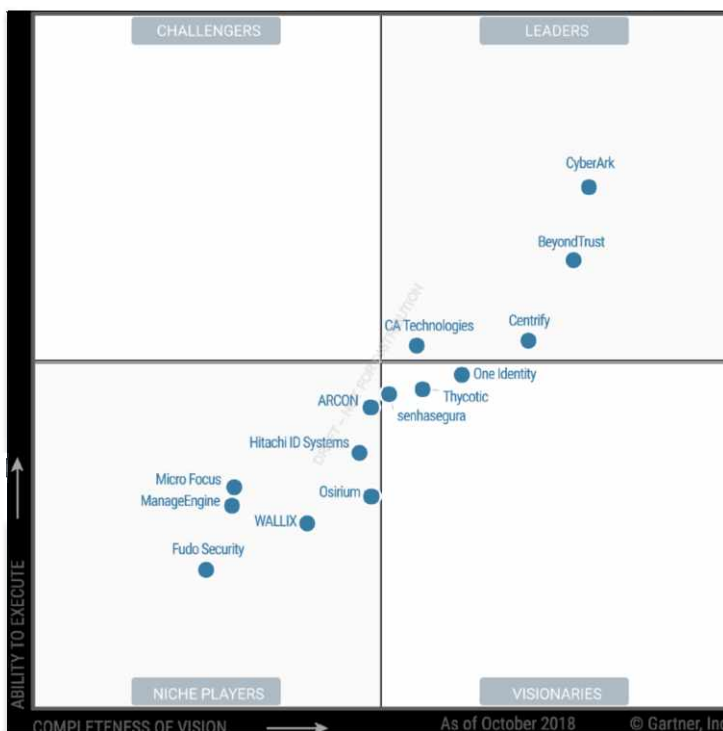
Nabízené řešení plně splňuje požadavky zadavatele uvedené v zadávací dokumentaci a upřesňujících dotazech.

### 6.1 Popis řešení pro PAM

Nabízený systém od společnosti BeyondTrust Corporation je světovým lídrem v oblasti správy privilegovaných přístupů (PAM) a poskytuje nejplynulejší přístup k prevenci narušení dat souvisejících s odcizenými přihlašovacími údaji, zneužitými oprávněními a nezabezpečeným vzdáleným přístupem.

BeyondTrust poskytuje organizacím viditelnost a kontrolu, kterou potřebují ke snížení rizika, dosažení cílů v souladu se zvýšením provozní výkonnosti. Důvěřuje jim více než 20 000 zákazníků po celém světě, včetně více než poloviny z žebříčku Fortune 500, včetně 9 z 10 nejprestižnějších značek na světě dle Forbes. Disponuje více než 14 pobočkami v různých zemích světa a nabízí platformu pro řízení privilegovaných účtů s nejširším pokrytím všech zákaznických potřeb.

Dle níže uvedeného Gartner Magic Quadrant z roku 2018 je patrné, že po fúzi se společností Bomgar předstihne i v tomto hodnocení dosavadního lídra CyberArk a bude tak na prvním místě.



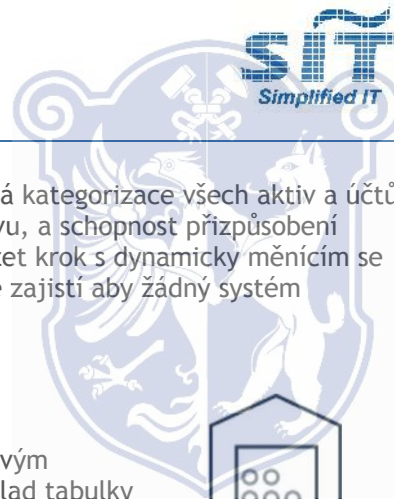
### BeyondTrust Password Safe

Naše řešení pomáhá bezpečnostním týmům překonat rizika plynoucí ze zmíněných tradičních přístupů k vytváření, správě a používání citlivých administrátorských přihlašovacích údajů těmito pokročilými funkcemi:

#### Automatická detekce účtů

Naše řešení Password Safe využívá zabudovaný skenovací engine nástroj pro skenování,





identifikaci a profilování všech aktiv a privilegovaných účtů v síti. Dynamická kategorizace všech aktiv a účtů umožňuje proces automatického zahrnování účtů a aktiv pod centrální správu, a schopnost přizpůsobení přístupových politik změnám v prostředí. Tato funkcionalita pomáhá IT udržet krok s dynamicky měnícím se prostředím organizace a snižuje časovou a administrativní náročnost tím, že zajistí aby žádný systém nezůstal nemonitorovaný/nespravovaný.

### Centrální zabezpečené úložiště hesel

Šifrované úložiště slouží jako centralizované a kontrolované místo a je klíčovým řešením pro eliminaci nebezpečných metod ukládání hesel (jako jsou například tabulky aplikace Excel), které usnadňují sdílení a vyzrazení přihlašovacích údajů. Naše řešení obsahuje úložiště se šifrováním odpovídajícím standardu FIPS 140-2 -> AES.



### Bezpečné použití hesel + SSO (Single-Sign-On)

Uložení přihlašovacích údajů k privilegovaným účtům do sejfů je zbytečné, pokud neexistuje způsob jejich bezpečného získání a použití. Prvním krokem tohoto procesu je silné ověření entity (ať už osoby, aplikace nebo skriptu), která se snaží uložené přihlašovací údaje použít. Řešení následně předá uložené přihlašovací údaje oprávněné entity (uživatelé nebo aplikace) přímo cílovému systému. Oproti běžným řešením typu „uložit/vyzvednout“ v tomto případě uživatel svá hesla vůbec nezná, neuvidí a ani nezíská a tím se výrazně snižuje riziko jejich vyzrazení. Navíc protože ověření na cílovém systému je plně automatické, a uživatelé si tedy nemusí pamatovat ani přepisovat svá hesla, je možné nastavit politiky s výrazně vyššími požadavky na složitost hesel a umožnit funkcionalitu SSO kdy má uživatel pouze jedno přihlašovací jméno a heslo, kterým se autentizuje vůči systému, bez znalosti přístupových údajů na koncové systémy.



### Aplikace - Aplikace (A2A) management hesel

Jak již bylo zmíněno, lidé nejsou jedinými uživateli privilegovaných přihlašovacích údajů. Ve většině organizací mohou mít k citlivým prostředkům, například aplikacím nebo databázím, přístup také různé skripty a aplikace. Proto řešení Password Safe nabízí v rámci správy aplikačních hesel i tyto funkcionality:



- Umožňuje odebrání hard-coded hesel z aplikací a skriptů.
- Poskytuje rozšiřitelné rozhraní REST, které podporuje mnoho programovacích jazyků, včetně C / C + +, Perl .NET a Java.
- Zajišťuje automatické resetování hesel při uvolnění.
- Vynucuje rozsáhlé ovládací prvky zabezpečení pro uzamčení přístupu pouze k autorizovaným aplikacím.

### Bezpečná správa SSH klíčů

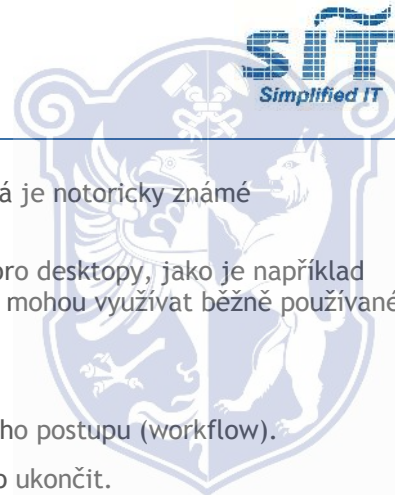
Kromě podpory šifrování se také mnoho klíčů používá pro ověření identity držitele. Ačkoli tyto klíče nejsou hesly v tradičním smyslu, fungují velmi podobně a jsou vystaveny také podobným rizikům a hrozbám, jako jsou kopírování, sdílení, nechtěné prozrazení a neauditovaná zadní vrátka. Protože se tyto klíče často vkládají přímo do kódu nebo jsou používány transparentně, aby uživatelé nebyli zatěžováni jejich relativní složitostí, jsou také více ohroženy zastaráním nebo zcizením. Proto logicky naše řešení umožňuje na tyto klíče uplatnit stejné postupy, které jsou používány pro správu a ochranu hesel.



### Bezagentský management privilegovaných session

Monitorování a správa privilegovaných relací je nezbytné pro dosažení shody s předpisy (Compliance) a bezpečnostních politik organizace. Může však být velice





složitá a časově náročná. Mnoho alternativ na trhu nutí používat Javu, která je notoricky známé bezpečnostní riziko.

Password Safe privileged session management používá standardní nástroje pro desktopy, jako je například PuTTY a Microsoft Terminal Services klient, což zajišťuje, že administrátoři mohou využívat běžně používané nástroje pro správu bez potřeby Javy. Administrátoři mohou:

- Požadovat pouze přístup RDP / SSH k jim autorizovaným systémům.
- Spustit relace okamžitě nebo prostřednictvím schváleného pracovního postupu (workflow).
- Zobrazit si aktivní relace a v případě potřeby relaci pozastavit nebo ukončit.
- Používat keystroke indexování a fulltextové vyhledávání tak, aby vyhledali požadovaná data s automatickým ukládáním logů o přehraných relacích pro pozdější účely auditu.
- Vyhněte se Javě - Password Safe je bezklientské řešení bez nutnosti instalace agentů na koncové servery.
- Plně integrovat s nativními nástroji (MSTSC, PuTTY, MobaXterm atd.).
- Získejte kompletní videozáznam se 100% odpovědností a auditovatelností.

## 6.2 Požadavky na součinnost PAM

### 6.2.1 Prostředí

Na straně zadavatele je nutné připravit vhodnou infrastrukturu tak, aby bylo možné spustit PasswordSafe instance:

Existují dvě možnosti implementace:

#### 1) Import VMware image:

**Hardware:** Doporučený: Intel Dual Core 2 GHz, 64-bit procesor (nebo kompatibilní, minimum)

**Operační paměť:** Minimum: 16 GB  
Doporučená: 32 GB

**Disk:** 330 GB

**VMware:** ESX verze: 5.5, 6.0, 6.5  
vSphere Windows client: 5.5, 6.0  
vSphere Web client: 6.0, 6.5

**Důležité:** Po importu image (před startem systémů) je doporučeno udělat snapshot.

#### 2) Import Hyper-V image:

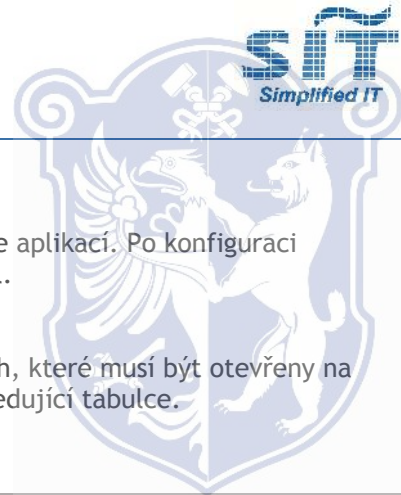
**Hardware:** Doporučený: Intel Dual Core 2 GHz, 64-bit procesor (nebo kompatibilní, minimum)

**Operační paměť:** Minimum: 16 GB  
Doporučená: 32 GB

**Disk:** 330 GB

**Hyper-V:** Hyper-V 2016 nebo vyšší

**Důležité:** Po importu image (před startem systémů) je doporučeno udělat snapshot.



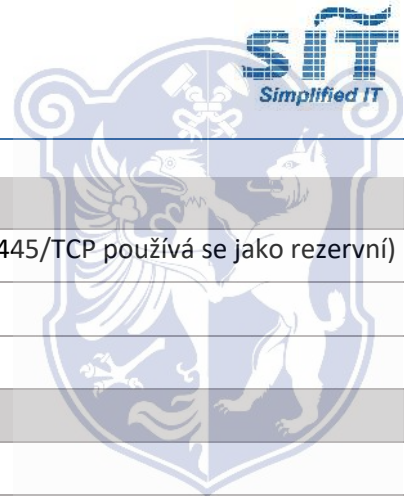
## 6.2.2 Terminálový server

Zadavatel dodá Terminálový Server pro případné účely vzdálené konfigurace aplikací. Po konfiguraci Terminálového Serveru budou přidány aplikace dostupné skrze RDP protokol.

### Porty

Systém Password Safe vyžaduje správnou komunikaci na konkrétních portech, které musí být otevřeny na obou apliancích. Seznam požadovaných otevřených portů je popsán v následující tabulce.

Funkce	Služba	Porty	Protokol
Uživatelské rozhraní	https	443	TCP
Remote Desktop	rdp	4489	TCP
SSH	ssh	4422	TCP
Počet uživatelů	nb-ssn   ms-ds	139   445	TCP (preferované 445)
Počet zařízení	nb-ssn   ms-ds	139   445	TCP (preferované 445)
Počet softwaru	nb-ssn   ms-ds	139   445	TCP (preferované 445)
Místní skenovací služby	ms-ds	445	TCP
<b>Zařízení</b>			
Checkpoint	ssh	22	TCP
Cisco	ssh	22	TCP
Dell iDRAC	ssh	22	TCP
F5 BIG IP	ssh	22	TCP
HP Comware	ssh	22	TCP
HP iLo	ssh	22	TCP
Juniper	ssh	22	TCP
Palo Alto	ssh	22	TCP
Fortinet	ssh	22	TCP
SonicWall	ssh	22	TCP
AIX	ssh	22	TCP
HP-UX	ssh	22	TCP
IBMi (AS400)	telnet	23	TCP
Linux	ssh	22	TCP
MAC OSX	ssh	22	TCP
Solaris	ssh	22	TCP
Windows Desktop	ads-i-ldap	389	TCP (ms-ds 445/TCP používá se jako rezervní)
Windows Server	ads-i-ldap	389	TCP (ms-ds 445/TCP používá se jako rezervní)
Windows Update / Restart Services	wmi	135	TCP (Služba WMI pracuje na cílovém systému)



<b>Directories</b>			
Active Directory	ads-ildap	389	TCP (ms-ds 445/TCP používá se jako rezervní)
RACF	ssh	22	TCP
LDAP/S	ldap	389	TCP
<b>Databáze</b>			
Oracle	oracle-listener	1521	TCP
MS SQL Server	netlib	1433	TCP
Sybase ASE		5000	TCP
MySQL		3306	TCP
Teradata		1025	TCP
<b>Aplikace</b>			
Vmware vSphere API		API	
Vmware vSphere SSH		22	TCP
SAP		API	
<b>Řízení relací</b>			
Remote Desktop	rdp	3389	TCP
SSH	ssh	22	TCP
<b>Appliance BeyondTrust</b>			
Mail Sever Integrace	smtp	25	TCP
Integrace s AD	ldap	389	TCP
Backup	smb	445	TCP
Time Protocol	ntp	123	TCP
Replikace HA	sql-mirroring https	5022 443	TCP
Radius	radius	1812 1813	UDP
<b>Other</b>			
Syslog	syslog	514 6514	TCP, UDP

Přístup do internetu pro aktivaci licence a aktualizace (jednodušší správa a instalace)



## Pravidla pro tvorbu hesel

Potřebujeme znát pravidla pro tvorbu hesel, tedy požadavky na komplexitu hesla nastavené na systémech, které mají být pod správou Password Safe. Nejedná se o politiku hesel stanovenou organizací ve směrnici, jedná se o skutečné nastavení a vynucení politik na systémech.

Systém Password Safe vyžaduje nastavení pravidel tvorby hesel, velmi pravděpodobně bude nutné pro různé typy systémů připravit specifická pravidla tvorby hesel, nejméně však jedno, pokud je aplikovatelné obecně v organizaci. Pravidla definovaná v Password Safe musí být mnohem restriktivnější než pravidla v systémech, aby se zamezilo neúspěšným změnám hesla, kdy heslo automaticky vygenerované v Password Safe nesplní pravidla definovaná na daném systému nebo v doméně a dojde k chybě při změně hesla v řízeném systému. Obrázek ukazuje screenshot z nastavení pravidla v Password Safe

Minimum and Maximum Characters    Min: 4    Max: 128

Uppercase Requirements     Not Permitted  
 Permitted, not required  
 Required

Valid Uppercase Requirements    ABCDEFGHIJKLMNOPQRSTUVWXYZ

Lowercase Requirements     Not Permitted  
 Permitted, not required  
 Required

Valid Lowercase Requirements    abcdefghijklmnopqrstuvwxyz

Numeric Requirements     Not Permitted  
 Permitted, not required  
 Required

Non-Alphanumeric Requirements     Not Permitted  
 Permitted, not required  
 Required

Valid Non-Alphanumeric Characters     All

~     &     ?     {  
 !     \*     /     }  
 @     (     <     \_  
 #     )     >     .  
 \$     -     |  
 %     +     [  
 ^     =     ]



### Vzdálený nebo fyzický přístup pro instalaci systému

Instalaci a konfiguraci Beyond Trust není možné provádět přímo z appliance a je potřebný alespoň jeden počítač s instalací Adobe Flash player případně prohlížeč Chrome (obsahující Flash player). Lze nahradit VPN přístupem a instalaci z počítače dodavatele.

### Informace uživateli při logování do BeyondTrust

Text, nebo také varování, které je zobrazeno před přihlášením uživatele do BeyondTrust, tzv. login banner

### Zálohování

Síťová složka (NFS), kam bude možné ukládat zálohy, tato složka by měla být pravidelně zálohována nejlépe na pásku, uživatelské jméno a heslo pro přístup na složku (účet)

### Role pro uživatele a správu PAM

Připravit v Active Directory případně v LDAP adresářové službě, bezpečnostní skupiny (role) naplněné uživateli, kteří budou oprávněni administrovat PAM, doporučujeme připravit také role pro uživatele (administrátory) dle jednotlivých systémů (windows, linux, middleware, DevOps, Extrernisté a jiné.), pokud je procesně vyžadováno i schvalování či auditování přístupů, tak i role k tomuto účelu.

Připravit účet v adresářové službě pro ověření uživatelů přes adresářovou službu.

### Funkční účty pro automatickou správu privilegovaných účtů na systémech a doméně

Připravit v Active Directory a v systémech účty které budou použity k napojení systémů do PAM. Tyto účty musí mít dostatečné oprávnění k řízení ostatních účtů na daném systému.

### Zasílání logů k vyhodnocení v monitorovacích systémech

BeyondTrust umí zasílat logy k vyhodnocení provozními a bezpečnostními nástroji, pokud je vyžadováno, je potřeba dodat IP adresy a požadovaný formát logu TCP/UDP/TCP-SSL, pro zasílání aplikačních logů.

### Ostatní doporučení, známá omezení

Nedoporučuje se zapojovat BeyondTrust appliance do domény a aplikovat externí politiky.

Není vhodné instalovat software třetích stran na BeyondTrust appliance.

Aktualizace a instalace bezpečnostních záplat operačního systému a databáze vyžaduje zvláštní přístup a není možné jej automatizovat.



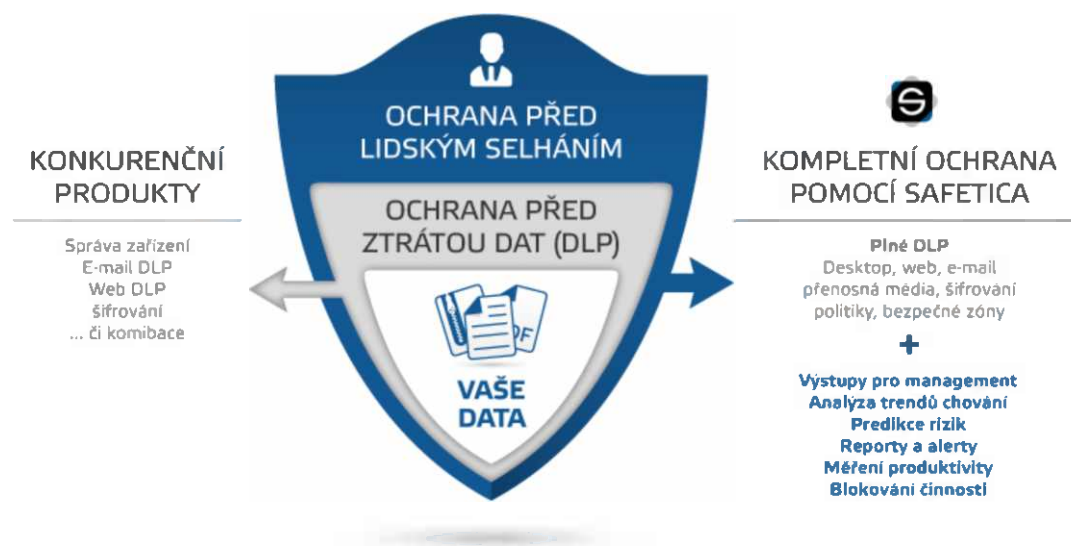


### 6.3 Popis řešení pro zavedení DLP

Software Safetica je kompletní řešení vnitřní bezpečnosti, které přináší změnu ve vnímání rizik. Zatímco ostatní hovoří o datech a ochraně soustředěně 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 hrozcích 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 posílání souborů
- Kopírování na osobní zařízení
- Krádež/ztráta zařízení (notebook, pevný disk, tablet, mobil)
- Upload na cloudové úložiště
- Rizika BYOD
- Vydírání 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 nebo tiskem.



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



**Vysoká ochrana proti oobejtí,** 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 vzdělávat uživatele 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 stránkám. 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 nepovoláný 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)
- Využití 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

### Požadavky na funkcionalitu dle zadání VŘ:



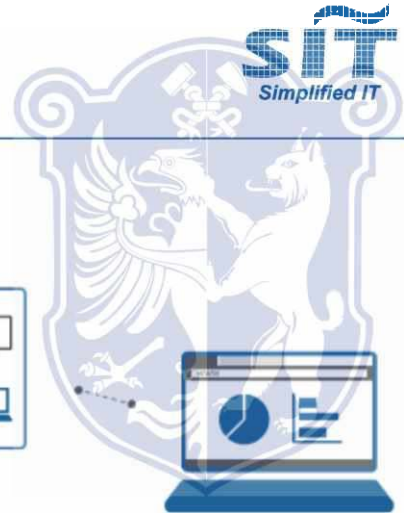
Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Všeobecné požadavky		
Integrace s Microsoft Active Directory.	Ano	Ano
Podpora databázového serveru MS SQL 2008 a novější	Ano	Ano
Podpora OS Windows 7 a vyšší	Ano	Ano
Podpora OS Windows Server 2008 R2 a vyšší	Ano	Ano
Podpora terminálového prostředí (RDP, Citrix)	Ano	Ano
Centrální administrativní konzole s přizpůsobením.	Ano	Ano
Možnost auditu přístupu k výsledkům a nastavením produktu, řízení přístupových oprávnění k administraci.	Ano	Ano
Skrytý režim vč. skrytí procesu a složek, a to i vzhledem k lokálnímu nebo doménovému administrátorovi přítomnému na koncové stanici.	Ano	Ano
Ochrana proti obejití systému	Ano	Ano
Ochrana systému proti obejití musí být aktivní pro uživatele, lokálního i doménového administrátora.	Ano	Ano
Nemožnost zastavit procesy, v případě zvýšených práv automatické obnovení nebo jiná ochrana.	Ano	Ano
Nemožnost odinstalace bez explicitní autorizace.	Ano	Ano
Nemožnost změny registru, zásahu do komponent systému, knihoven DLL.	Ano	Ano
Nemožnost měnit nastavení z koncové stanice.	Ano	Ano
Musí existovat řešení pro ochranu v nouzovém režimu (safe mode).	Ano	Ano
Funkčnost musí přetrvávat také v tzv. offline režimu mimo připojení do firemní sítě nebo na internet.	Ano	Ano
Možnost práce s historickými daty.	Ano	Ano
Řešení musí podporovat nebo přímo poskytovat zálohování vlastních komponent, zejména záznamů a konfigurace.	Ano	Ano
Generování automatických emailových zpráv v případě vzniku incidentu, umožnit přizpůsobit prahy citlivosti i specifikaci incidentu.	Ano	Ano
Generování automatických reportů do emailu s možností je plně přizpůsobit (množství informací, okruh sledovaných uživatelů, četnost odesílání a adresáty).	Ano	Ano
Možnost posílání záznamů do SIEM systému.	Ano	Ano
MDM řešení pro Android, iOS a Windows Phone	Ano	Ano
Bezpečnostní audit:		
Podrobné informace o době spuštění a rovněž o době skutečně aktivního využívání konkrétních aplikací, tyto jsou zároveň pro	Ano	Ano



Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
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.	Ano	Ano
Možnost exportu záznamů do XLS, PDF.	Ano	Ano
Instant Messenger aplikace, webový email – možnost monitorování odeslaných dat nezávisle od typu aplikace nebo služby.	Ano	Ano
E-mail:		
Podpora protokolů POP3, IMAP, MAPI / Exchange včetně šifrování SSL.	Ano	Ano
Podpora emailového klienta MS Outlook, Thunderbird, Icewarp atd. – řešení je schopné monitorovat e-mailové aplikace, nezávisle na typu aplikace.	Ano	Ano
Pohyb dat:	Ano	
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.	Ano	Ano
Lokální operace se soubory – kopírování, přesun, stažení z webu, FTP, mazání, vytváření, otevírání včetně identifikace zdrojové a cílové lokality – cesta, typ zařízení, jednoznačný identifikátor.	Ano	Ano
Logování vytištěných dat.	Ano	Ano
Použití kopírování do schránky a snímání obrazovky.	Ano	Ano
Aktivita na stanici:		
Log zapnutí/vypnutí PC.	Ano	Ano
Log přihlášení/odhlášení uživatele.	Ano	Ano
Log spánku/vzbuzení PC.	Ano	Ano
Síťová aktivita:		
Objem stažených a zaslaných dat.	Ano	Ano
Ochrana dat:		
Nezávislost na aplikaci, protokolu vč. šifrovaného spojení.	Ano	Ano
Řešení je odolné vůči obejití ochrany na souborovém systému při použití odkazů na jiné složky včetně symbolických odkazů a podobných technologií.	Ano	Ano
Šifrování:		
Šifrování celých disků (Full Disk Encryption) i pro systémové disky.	Ano	Ano



Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Šifrování USB flash disků.	Ano	Ano
Virtuální šifrované disky	Ano	Ano
Vynucení šifrování v předem definovaných akcích (zasílání dat na neautorizovaná úložiště)	Ano	Ano
Data Loss Prevention	Ano	Ano
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	Ano	Ano
Možnost monitorovacího, upozorňovacího i zakazovacího režimu.	Ano	Ano
Možnost navázání politik na konkrétní aplikace – definice zdrojů (konkrétní data, přístup k externím zařízením, síti), které aplikace může využít pro svůj běh.	Ano	Ano
Device Control	Ano	Ano
Globální omezení na USB, firewire, paměťové karty, LPT, COM, Bluetooth, CD, DVD, Blue-ray.	Ano	Ano
Možnost read-only módu.	Ano	Ano
Auditní záznam veškerých externích zařízení připojovaných do systému vč. monitoru, klávesnic a myši.	Ano	Ano



## Architektura řešení



PC, notebooky, mobily a tablety s instalovaným **Safetica klientem**

Klient na koncové stanici zaznamenává aktivitu a **vynučuje bezpečnostní politiku** nad firemními daty. Lze jej skrýt před uživatelem

**Server** a databáze

Získané informace jsou přenášeny na server. Data z notebooků se přenesou ihned po připojení do sítě. V opačném směru je šířena aktualizace nastavení klientů

**Desktopová Safetica** s výstupy a nastavením

Získaná data lze zobrazit v **jednotné konzoli**. Veškeré nastavení je prováděno tamtéž

**WebSafetica**

Analytický nástroj WebSafetica poskytuje online přehledy získaných dat. Běží v každém prohlížeči, na počítači i mobilu

### 6.3.1 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):

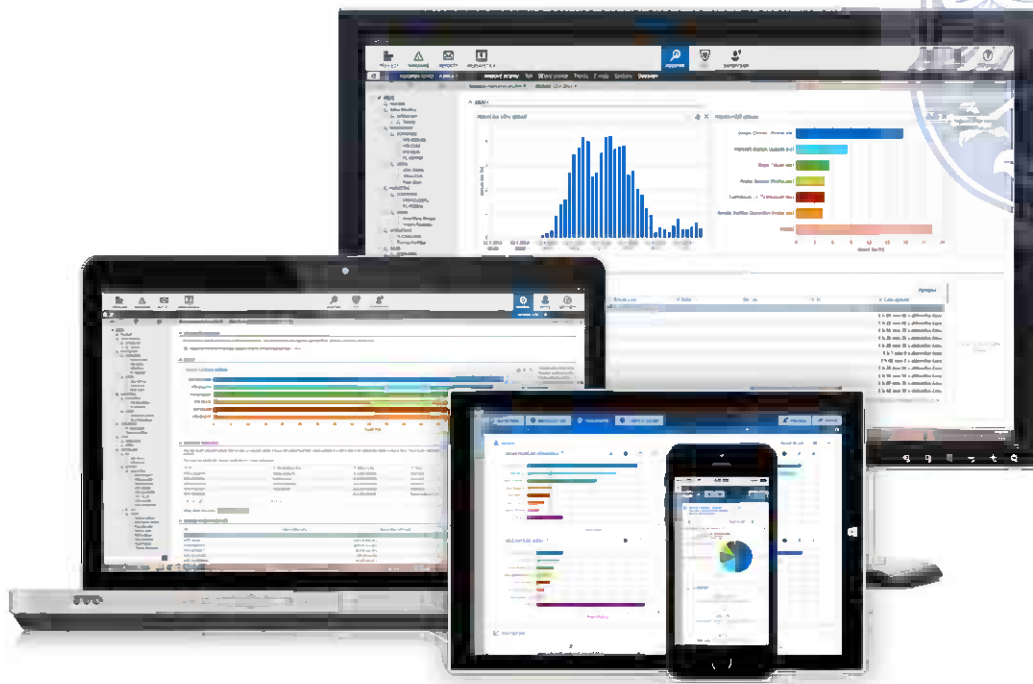
- Požadavky dle edice MS SQL
- Sdílený nebo dedikovaný server, doporučujeme min. 100GB volného místa na disku
- MS SQL 2008 R2 a vyšší, případně MS SQL 2012 Express a vyšší (verze zdarma)
- MS SQL 2012 Express je volitelná součást instalátoru



Nabídka: „Dodávka a implementace vybraných nástrojů kybernetické bezpečnosti Statutárního města Kladno - Nástroje kybernetické bezpečnosti“



Ukázka Safetica





## 6.4 Plán implementace Safetica

Nainstalovat software Safetica do prostředí zákazníka dle smlouvy o dílo

Nastavit software Safetica na základě konzultace / bezpečnostní analýzy a tím docílit zvýšení datové bezpečnosti ve společnosti

### 6.4.1 Harmonogram projektu

Začátek projektu

Fáze projektu	Předpokládané trvání
1. Instalace	1 týden od kick-off meetingu
2. Monitorovací období	4 týdny od akceptace fáze 1
3. Analýza sesbíraných dat	Přibližně 1 týden od akceptace fáze 2
4. Školení	(součástí ostatních fází)
5. Konfigurace DLP	5 týdnů od akceptace fáze 3

### 6.4.2 Podmínky pro implementaci produktu

Objednatel je zodpovědný za zajištění následovných podmínek pro implementaci:

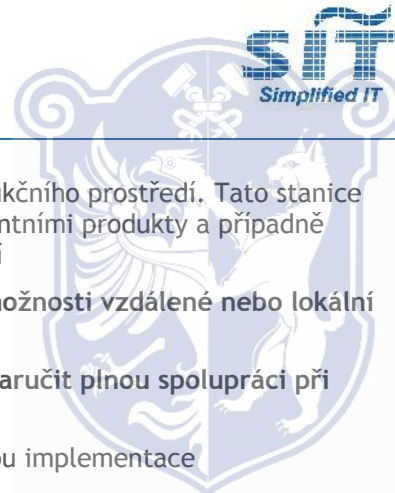
Zajistit splnění všech **hardwarových** a **softwarových** podmínek pro instalaci databáze Microsoft® SQL Server (2012 a vyšší), Safetica Management Service, Safetica Management Console, WebSafetica, Safetica Agent, Safetica Endpoint Client na relevantních stanicích z požadovaného rozsahu implementace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

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“

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 stanice** (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

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

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

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

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“

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**

### 6.4.3 Fáze projektu

#### 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.



**Příloha č. 2 – Položkový rozpočet**

<b>Počáteční investice</b>			
Specifikace	bez DPH (Kč)	sazba DPH (Kč)	Cena včetně DPH (Kč)
Dodávka SW - Centrální správa privilegovaných účtů (instalace, testovací provoz)	18 000 Kč	3 780 Kč	21 780 Kč
Licence	3 586 000 Kč	753 060 Kč	4 339 060 Kč
Integrace se stávajícími IS úřadu	6 000 Kč	1 260 Kč	7 260 Kč
Dodávka SW - DLP (instalace, testovací provoz)	12 000 Kč	2 520 Kč	14 520 Kč
Licence	1 241 550 Kč	260 726 Kč	1 502 276 Kč
Integrace se stávajícími IS úřadu	6 000 Kč	1 260 Kč	7 260 Kč
Zaškolení administrátorů*	6 000 Kč	1 260 Kč	7 260 Kč
<b>Cena počáteční investice</b>	<b>4 875 550 Kč</b>	<b>1 023 866 Kč</b>	<b>5 899 416 Kč</b>

\* Zaškolení v rozsahu 20 hodin minimálně pro 5 pracovníků Zadavatele

<b>Servisní podpora na dodané dílo v délce trvání 60 měsíců od spuštění do ostrého provozu</b>			
Specifikace	bez DPH (Kč)	sazba DPH (Kč)	Cena včetně DPH (Kč)
Cena započaté hodiny	-----	-----	-----
Cena provozních nákladů za 60 měsíců	2 520 000 Kč	529 200 Kč	3 049 200 Kč

<b>Servisní zásahy nad rámec záruky a havárie **</b>			
Specifikace	bez DPH (Kč)	sazba DPH (Kč)	Cena včetně DPH (Kč)
Cena započaté hodiny	1 250 Kč	263 Kč	1 513 Kč

\*\* Cena za 1 hodinu servisního zásahu nesmí překročit 1.300,-Kč bez DPH a celkové servisní náklady za 60 měsíců mohou činit maximálně 800.000,-Kč bez DPH.

<b>Náklady na rozvoj, provoz, servisní zásahy a havárie na dobu 10 let (6. až 15. rok) ***</b>			
Specifikace	bez DPH (Kč)	sazba DPH (Kč)	Cena včetně DPH (Kč)
Cena započaté hodiny servisního zásahu	1 250 Kč	263 Kč	1 513 Kč

\*\*\* Náklady po ukončení doby udržitelnosti projektu na dobu 10 let (6. až 15. rok), mohou činit maximálně 3.000.000,-Kč bez DPH a cena za 1 hodinu práce nesmí překročit 1.300,-Kč bez DPH.



EVROPSKÁ UNIE  
Evropský fond pro regionální rozvoj  
Integrovaný regionální operační program



MINISTERSTVO  
PRO MÍSTNÍ  
ROZVOJ ČR



**Příloha č. 3** – Podrobný nabídkový rozpočet (z nabídky ve veřejné zakázce)

Účastník zde vloží Podrobný nabídkový rozpočet ze své nabídky *předložené ve veřejné zakázce.*





**Příloha č. 3 – Podrobný nabídkový rozpočet (z nabídky ve veřejné zakázce)**

Účastník zde vloží Podrobný nabídkový rozpočet ze své nabídky předložené ve veřejné zakázce.

**Podrobný nabídkový rozpočet pro část 2 "Nástroje kybernetické bezpečnosti"**

Zařízení	Počet	Cena za 1 ks (v Kč bez DPH)	Cena celkem (v Kč bez DPH)	DPH (%)	Cena celkem (v Kč vč. DPH)
<b>Nástroj pro řízení přístupových oprávnění</b>			<b>3 610 000 Kč</b>		<b>4 368 100 Kč</b>
Licence (multilicence)	1	3 586 000 Kč	3 586 000 Kč	21%	4 339 060 Kč
Instalační a implementační práce	1	6 000 Kč	6 000 Kč	21%	7 260 Kč
Hardware (server) pro řízení přístupových oprávnění	1	0 Kč	0 Kč	21%	0 Kč
Pilotní provoz	1	6 000 Kč	6 000 Kč	21%	7 260 Kč
Dokumentace	1	6 000 Kč	6 000 Kč	21%	7 260 Kč
Školení	1	6 000 Kč	6 000 Kč	21%	7 260 Kč
<b>DLP (Data Loss Prevention)</b>			<b>1 265 550 Kč</b>		<b>1 531 316 Kč</b>
Licence (multilicence)	1	1 241 550 Kč	1 241 550 Kč	21%	1 502 276 Kč
Instalační a implementační práce	1	6 000 Kč	6 000 Kč	21%	7 260 Kč
Pilotní provoz	1	6 000 Kč	6 000 Kč	21%	7 260 Kč
Dokumentace	1	6 000 Kč	6 000 Kč	21%	7 260 Kč
Školení	1	6 000 Kč	6 000 Kč	21%	7 260 Kč
<b>NABÍDKOVÁ CENA ZA POČÁTEČNÍ INVESTICE</b>			<b>4 875 550 Kč</b>		<b>5 899 416 Kč</b>
<b>Provozní náklady</b>	<b>Počet</b>	<b>Cena za 1 ks (v Kč bez DPH)</b>	<b>Cena celkem (v Kč bez DPH)</b>	<b>DPH (%)</b>	<b>Cena celkem (v Kč vč. DPH)</b>
Provozní náklady (měsíční) - Nástroj pro řízení přístupových oprávnění	60	21 000 Kč	1 260 000 Kč	21%	1 524 600 Kč
Provozní náklady (měsíční) - DLP (Data Loss Prevention)	60	21 000 Kč	1 260 000 Kč	21%	1 524 600 Kč
<b>NABÍDKOVÁ CENA ZA PROVOZNÍ NÁKLADY ZA 60 MĚSÍCŮ</b>			<b>2 520 000 Kč</b>		<b>3 049 200 Kč</b>



Příloha č. 4 - Závazný harmonogram plnění

Účastník zde vloží závazný harmonogram plnění ze své nabídky předložené ve veřejné zakázce.

Etapa Činnost	Předpokládaná doba trvání etap												
	Týden 1	Týden 2	Týden 3	Týden 4	Týden 5	Týden 6	Týden 7	Týden 8	Týden 9	Týden 10	Týden 11	Týden 12	
I Diskuze o nástroji a upřesnění rozsahu.	■												
II Příprava předimplementační dokumentace.		■											
III Nachystání prostředí dle analýzy ze strany zákazníka			■										
IV Instalace a konfigurace UVM aplikace.				■									
V Přidání jednotlivých systémů a privilegovaných účtů do spravy systému PAM.					■								
VI Akceptační testy								■					
VII Školení uživatelů a systémových administrátorů.										■			
VIII Vpracování dokumentace a pokynů.												■	