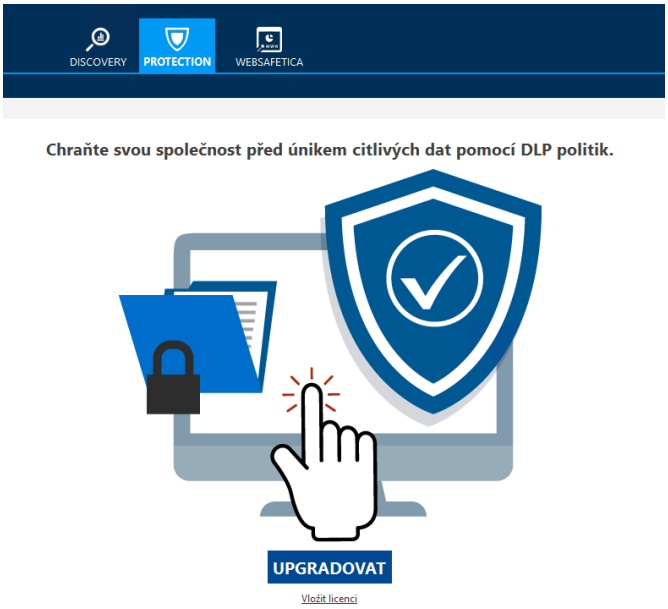
Název veřejné zakázky: **KYBEZ města Litvínov – upgrade licence Safetica**

systémové číslo: P24V00000107

# 1. Předmět veřejné zakázky

Předmětem veřejné zakázky je rozšíření funkcí aktuálně používané aplikace Safetica o funkce DLP, a to prostřednictvím dodávky licence Safetica Protection PERPETUAL pro 210 koncových stanic vč. maintenance na dva roky.




# 2. Popis stávajícího prostředí

V současné době vlastní MěÚ Litvínov licenci Safetica Auditor PERPETUAL pro 210 koncových stanic. Jedná se tedy o licenci trvalou, ke které je sjednána služba maintenance, díky čemuž je zajištěna aktuálnost verze. Aktuálně MěÚ Litvínov provozuje jednu serverovou instanci Safetica ve verzi 10.5.10.

Registrované ID zákazníka je 1855f263-0d99-403d-9e0b-b53fff166a20

# 3. Požadované parametry technického řešení

MěÚ Litvínov chce povýšit svou úroveň kybernetické bezpečnosti o ochranu před únikem informací (DLP), čehož chce dosáhnout upgradem již provozované a ověřené aplikace Safetica. Vyšší verze aplikace Safetica musí splňovat minimálně tyto specifikace:

- Podpora terminálových prostředí.
- Centrální administrátorská konzole.
- Řízená uživatelská práva do nastavení konzole, k výsledným logům a administraci řešení.
- Skrytý režim na koncové stanici včetně procesů a složek, a to včetně lokálních i doménových administrátorů.
- Ochrana proti zastavení systému.
- Ochrana proti zastavení systému musí být aktivní u běžného uživatele, lokálního i doménového administrátora.

- Ochrana proti zastavení procesů; V případě vyšších uživatelských práv dojde k restartu zastavených procesů či k použití jiných způsobů pro obnovu služby.
- Ochrana proti odinstalaci řešení bez potřebné autorizace.
- Ochrana proti editaci registrů, systémových komponent či DLL knihoven.
- Ochrana proti změně nastavení na koncové stanici.
- Nutná ochrana proti přihlášení uživatele do operačního systému v režimu “safe mode”.
- Všechny funkcionality musí být zachovány i v offline režimu, např. když koncová stanice není připojena k firemní síti nebo k internetu.
- Možnost pracovat s historickými daty.
- Řešení musí podporovat možnost poskytnutí záloh vlastních komponent, převážně pak všech záznamů a nastavení.
- Automatické generování emailových varování v případě incidentů, možnost změnit citlivost a specifikace incidentu.
- Automatické generování emailových reportů s možností úprav obsahu (množství informací, množina uzlů, frekvence odesílání, příjemci).
- Detailní informace o aplikacích, jako čas spuštění a jejich aktivním využití. Aplikace jsou rozděleny do kategorií pro přehlednou správu.
- Detailní informace o webech, jako jejich aktivní využitím, informacích o URL, hlavičky webu, a to bez ohledu na použitý prohlížeč. Weby jsou rozděleny do kategorií pro přehlednou správu.
- Detailní informace o práci s citlivými soubory, např. přehled uživatelů a aplikací pracujících se soubory, souborové operace (otevření, přejmenování, kopírování, smazání atd.), a informace o cestách (systémové, externí, webové, cloudové atd.).
- Lokální souborové operace – kopírování, přesouvání, stahování z webu, FTP, smazání, vytvoření, otevření, a to včetně zdrojové a cílové identifikace: cesta, typ zařízení, jedinečný identifikátor.
- Zaznamenávaní tiskových úloh.
- Možnost exportu reportů do XLS, PDF.
- E-mail: POP3, IMAP, Exchange protokoly, včetně SSL šifrování.
- Podpora desktopových emailových klientů (Microsoft Outlook, Mozilla Thunderbird atd.) - řešení je schopno zaznamenávat e-maily nezávisle na použité klientské aplikaci.
- Podpora zaznamenávání souborů nahrávaných jako přílohy přes webové e-mailové klienty.
- Podpora zaznamenávání souborů odesílaných přes IM komunikační nástroje.
- Ochrana nezávisle na použitém SW, protokolu, včetně šifrovaných spojení.
- Řešení podporuje zabezpečení dat i v případě pokusu o porušení ochrany, např. pomocí symbolických odkazů na složku s daty apod.
- Šifrování celých disků včetně systémových.
- Šifrování externích USB disků.
- Restrikce pro USB mass storage zařízení, připojení mobilních telefonů, paměťové karty, Bluetooth přenosy souborů, optické disky či FireWire.
- Možnost vynucení režimu Pouze pro čtení u připojených zařízení.
- Zaznamenávání všech připojených zařízení včetně monitorů, myší a klávesnic.
- Schopnost blokovat pouze přenosy dat přes Bluetooth, ale povolit připojení a volné použití dalších Bluetooth zařízení (např. sluchátek)
- Klasifikovaná data lze chránit před zkopírováním na chytré telefony připojené přes Multimedia Transfer Protocol, tyto zařízení lze ale jinak neomezeně používat s necitlivými daty.

- Monitoring využití aplikací napříč organizací a možnost řídit, které aplikace lze a které nelze spouštět.
- Monitoring navštěvování webových stránek napříč organizací a možnost řídit, které webové stránky lze a které nelze navštěvovat.
- Definice kategorií citlivých dat dovoluje omezení pohybu a práce s těmito daty; určuje, která média mohou být použita pro přenos, které sítě mohou být použity pro upload, na které emailové adresy mohou být data odeslána, které aplikace mohou s daty pracovat.
- Možnost úplné blokace uživatelských akcí, uživatelského schválení operace, informativní notifikace uživatele či pouhého zaznamenání uživatelských akcí
- Možnost aplikace politik pro konkrétní aplikace – definice zdroje a cíle (přístup na externí zařízení, síť, tisk, virtuální tisk) a správa uživatelských operací (použití schránky, snímání obrazovky).
- Možnost správy či blokace nepovolených cloudových úložišť.
- Možnost správy či blokace přesouvání souborů do Git repozitářů.
- Funkcionalita „shadow copy“ umožňující administrátorovi prohlížení souborů, které byly součástí bezpečnostních incidentů. Funkce musí zpřístupnit soubory, které uživatel odeslal, i ty, které DLP řešení zablokovalo.
- Detekce citlivých dat v dokumentech na platformách Windows a macOS.
- Detailní přehled detekovaných citlivých dat v souboru, včetně počtu výsledků a jednotlivých nalezených výrazů a klasifikačních pravidel.
- Možnost definice citlivých dat pomocí předdefinovaných slovníků a algoritmů.
- Možnost definice citlivých dat pomocí vlastních řetězců či regulárních výrazů.
- Možnost importu vlastních slovníků klíčových slov.
- Možnost nastavení počtu výskytů citlivých údajů.
- Možnost ochrany heslem chráněných ZIP archivů vytvořených ze souborů s citlivým obsahem.
- Možnost klasifikace citlivých dat podle kontextových podmínek, např. původ nebo umístění dat.
- Možnost klasifikace kompatibilních typů souborů pomocí perzistentních souborových metadat.
- OCR vyhledávání citlivých dat v obrázkových formátech a skenovaných PDF dokumentech.
- OCR funkcionalita dostupná i když se počítače odpojí od firemní sítě nebo přepnou do offline režimu.
- OCR podpora pro dvoujazyčné prostředí (např. citlivé dokumenty v angličtině nebo v češtině)
- Dynamické restrikce nad soubory a aplikacemi při detekci citlivého obsahu.
- Blokace odeslání dat s citlivým obsahem mimo koncovou stanici – správa běžných komunikačních kanálů: e-mail, web upload, externí zařízení, IM komunikační nástroje, synchronizace s cloudovými aplikacemi.
- Detekce dat obsahujících citlivý obsah, uložených na koncové stanici nebo na sdíleném síťovém disku.
- Zaznamenávání běžných uživatelských akcí provedených na Office 365 cloudu (OneDrive, SharePoint Online) - základní souborové operace s cloudovými sobory, stahování a sdílení.
- Zaznamenávání Office 365 e-mailové komunikace (Exchange Online) pro všechny uživatele, včetně uživatelů pracujících z Outlook Web App, osobních nebo mobilních zařízení.
- Možnost automatického vytvoření DLP politik pro Office 365 e-mailovou komunikaci (Exchange Online) pro všechny uživatele, včetně uživatelů pracujících z Outlook Web App, osobních nebo mobilních zařízení.