Příloha 3 – Technická specifikace

Předpokládané počty zařízení:

- PC/Notebook **85** ks
- Mobilní zařízení - **50** ks

Aplikace, které kupující požaduje zahrnout do řízení bezpečnosti:

- Sdílení dokumentů v prostředí MS Windows Server
- MS Office 365
- DMS Alfresco Community Edition
- Spisová služba ICZ e-spis

Kupující poptává řešení v oblasti:

- Dodávka a implementace softwarového řešení poskytující účinnou ochranu proti úniku citlivých dat.
- Šifrování dat.
- Monitoring koncových stanic.
- Nastavení restriktivních opatření v oblasti citlivých dat.
- Reporting využívání koncových stanic.
- Spolupráce při implementaci.
- Technická podpora, aktualizace a nové verze veškerého dodaného SW budou poskytovány po dobu **4 let** od předání předmětu zakázky.

Obecné požadavky:

- Okamžitá ochrana dat - zabezpečení důležitých firemních dokumentů bez omezení provozu
- Přehled o aktivitách a činnosti na počítačích, síti a připojených zařízeních (Kompletní audit) – reporty, exporty, statistiky
- Stanovení a vynucení dodržování bezpečnostních pravidel, bezpečnostní audit a zamezení úniku dat z úřadu podle definovaných pravidel
- Snadné na použití – rychlé nasazení, správa všech zařízení (i externích) z jednoho místa. Jednotná konzole pro správu.
- Kompatibilita s Windows 10, integrace s Active Directory
- Automatické zálohování databáze
- Kompletní prevence úniků dat (DLP)
- Testovací a informativní DLP režimy
- Průběžná klasifikace nových a používaných dat
- Šifrování počítačů a externích zařízení (BitLocker na mass storage)
- Správa externích zařízení
- Analýza trendů a produktivity
- Blokování aplikací a webů
- Blokování citlivých e-mailových příloh
- Inspekce šifrovaných spojení SSL/HTTPS
- Soulad s ISO normami pro ochran dat
- Instalace a nastavení SW bude provedeno v rámci dodávky
- Správa mobilních zařízení (MDM pro iOS, Android)
- Možnost posílání záznamů do SIEM systému.

Bezpečnostní audit:

- Podrobné informace o době spuštění a rovněž o době skutečně aktivního využívání konkrétních aplikací, tyto jsou zároveň pro rychlé vyhodnocení tříděny do kategorií.
- Informace o skutečně aktivním čase jednotlivých webových stránek, včetně podrobných informací o URL, protokolu a titulku okna, nezávisle na použitém prohlížeči, tyto jsou zároveň pro rychlé vyhodnocení tříděny do kategorií.
- Možnost exportu záznamů do XLS, PDF.
- Instant Messager aplikace, webový email - možnost monitorování nezávisle od typu aplikace nebo služby.

Příloha 3 – Technická specifikace

Pohyb dat:

- Podrobné informace o práci s citlivými soubory jako kdo k těmto přistupoval, v jakých aplikacích s nimi pracoval, kam je ukládal, přejmenování a mazání, včetně externích zařízení, emailů a cloudových úložišť vč. synchronizované složky na disku.
- Lokální operace se soubory - kopírování, přesun, stažení z webu, FTP, mazání, vytváření, otevírání včetně identifikace zdrojové a cílové lokality-cesta, typ zařízení, jednoznačný identifikátor.
- Logování vytištěných dat.
- Použití kopírování do schránky a snímání obrazovky.

Aktivita na stanici:

- Log zapnutí/vypnutí PC.
- Log přihlášení/odhlášení uživatele.
- Log spánku/vzbuzení PC.

Síťová aktivita:

- Objem stažených a zaslaných dat.

Ochrana dat:

Obecně:

- Nezávislost na aplikaci, protokolu vč. šifrovaného spojení.
- Řešení je odolné vůči obejití ochrany na souborovém systému při použití odkazů na jiné složky včetně symbolických odkazů a podobných technologií.

Šifrování:

- Šifrování celých disků (Full Disk Encryption) i pro systémové disky.
- Šifrování složek a souborů.
- Vynucení šifrování v předem definovaných akcích (zasílání dat na neautorizovaná úložiště).
- Šifrování USB flash disků.

Data Loss Prevention:

- Pro definovaní kategorie citlivých dat mít možnost omezit pohyb a práci s daty - které média mohou být použity pro přenos, na jaký web může být provedeno nahrání souboru, na jakou emailovou adresu mohou být data zaslána; jaká aplikace může data otevřít.
- Možnost monitorovacího, upozorňovacího i zakazovacího režimu.
- Možnost navázání politik na konkrétní aplikace - definice zdrojů (konkrétní data, přístup k externím zařízením, síti), které aplikace může využít pro svůj běh.

Device Control:

- Globální omezení na USB, firewire, paměťové karty, LPT, COM, Bluetooth, CD, DVD, Blue-ray
- Možnost read-only módu.
- Auditní záznam veškerých externích zařízení připojovaných do systému vč. monitorů, klávesnic a myší.
- Mobilní telefony (Android, iOS, Windows Mobile):
    - Lokalizace.
    - Vzdálené zamknutí.
    - Smazání citlivých dat.
    - Reset do továrního nastavení
    - Management.