1. NÁZEV VEŘEJNÉ ZAKÁZKY

Název veřejné zakázky:	**UTB – Auditní systém pro Active Directory a souborové servery**

2. IDENTIFIKAČNÍ ÚDAJE ZADAVATELE

Obchodní název	**Univerzita Tomáše Bati ve Zlíně**
Sídlo:	nám. T. G. Masaryka 5555, 760 01 Zlín
IČ:	70883521
Statutární orgán:	prof. Ing. Vladimír Sedlařík, Ph.D., rektor

3. POPIS PŘEDMĚTU VEŘEJNÉ ZAKÁZKY

Předmětem plnění veřejné zakázky jsou:

1. Dodávka software pro audit síťového a souborového systému Active Directory provozovaného Zadavatelem;
2. Implementace software na současnou hardwarovou infrastrukturu ve vlastnictví Zadavatele;
3. Zaškolení administrátora v rozsahu 1 člověkoden;
4. Maintenance software na období 2 let.

4. DETAILNÍ TECHNICKÉ POŽADAVKY

Minimální požadavky

- Veškeré auditní zprávy a reporty musí být dostupné v aktuálním čase probíhajících událostí/změn.
- Audit koncových pracovních stanic musí být v rozsahu sledování alespoň: Logon/Logoff, Account Management, Vypnutí/Zapnutí, Souborová Integrita, Systémové události, použití USB.
- Ukládání auditních dat musí být v databázi MySQL, MS SQL, nebo PostgreSQL.

Auditní systém musí umožňovat:

- Sledování neaktivních, zakázaných uživatelských účtů a počítačů za účelem vyčištění prostředí Active Directory.
- Audit, monitorování a reporting nad kontroléry domény, včetně kompletní informace o změnách uživatelů, skupin, GPO, počítačů, práv a organizačních jednotek, DNS, schématu Active Directory a konfigurace.
- Audit času přihlášení a odhlášení z pracovních stanic uživatelů.
- Prohlížení a tvorbu harmonogramů grafických výkazů, s výstrahami zasílanými přes e-mail, z hlediska pravidelné analýzy a rychlé reakce na hrozby v oblasti bezpečnosti.
- Sledování přihlášení/odhlášení, tvorbu harmonogramů sledování událostí, aktivity terminálových služeb, času přihlášení a historie přihlašování.
- Kontrolu procesů auditu prostřednictvím sledování harmonogramu úkolů systému Windows.
- Ověření domény v rozsahu shody s normami, mj. SOX, PCI-DSS, které jsou spojeny se zajištěním efektivní kontroly bezpečnosti informací.
- Pravidelnou archivaci auditovaných údajů o událostech, prohlížení událostí z historie Active Directory, jako historie přihlašování uživatele, historie změn hesel, atd.

- Sledování událostí tvorby, úpravy a odstraňování souborů v důsledku povoleného a neautorizovaného přístupu, včetně detailní analýzy změn dokumentů, struktury jejich souborů, složek, účasti a oprávnění.
- Výstupní informaci o auditu a analýze přístupů k souborům a složkám obsahující minimálně údaje kdo je otevřel, smazal, přesunul, co, kdy a odkud.
- Monitoring integrity souborů, sledování změn souborů na serveru i lokálních systémových souborů a složek.
- Audit a reporting v souladu s regulačními nařízeními jako např. SOX, HIPAA, FISMA, GDPR, PCI, GLBA.
- Kompletní prohledávatelný audit všech souborových akcí (přístup/změna/smazání) v souborech a složkách na souborových serverech po libovolně nastavitelnou dobu bez požadavku na zapnuté nativní auditování souborových operací systémem Windows.
- Zobrazení dat přístupných určitému uživateli nebo skupině na souborových serverech.
- Monitorování vybraných kritických souborů a složek na souborových serverech Windows v reálném čase.
- Monitoring změn a přístupů na neomezený počet uživatelských adresářů a souborů souborových serverů objednatele.
- Automatické generování potřebných přehledů (reportů) ve stanovených časech.
- Export přehledů (reportů) minimálně ve formátech PDF, CSV.