

## **1. POPIS PLNĚNÍ PŘEDMĚTU ZAKÁZKY DODÁVKY SYSTÉMU PRO SPRÁVU HESEL**

Poptávané řešení bude sloužit pro správu přístupových oprávnění k systémům zadavatele, a to jak pro zaměstnance zadavatele, tak případné externí subjekty, které mají k těmto systémům mít přístup. Zároveň bude systém sloužit pro správu přístupových oprávnění zaměstnanců zadavatele k externím službám, ke kterým tito zaměstnanci přistupují v rámci svých pracovních povinností. Dále bude řešení zajišťovat automatizovanou výměnu hesel lokálních administrátorů na koncových stanicích Zadavatele.

Zadavatel poskytne pro implementaci systému potřebné virtuální stroje. Licence pro OS a případný další SW potřebný pro provoz systému musí být součástí dodávky.

Řešení musí zajistit funkčnosti popsané dále. V rámci této zadávací dokumentace, je heslem míněn libovolný řetězec znaků.

### **1. UKLÁDÁNÍ HESEL**

Řešení musí implementovat uložení hesel uživatelů tak, aby zajistilo, že přístup k heslům může získat pouze oprávněný uživatel. V rámci systému musí být možné ukládat různá hesla různými způsoby, tak aby byla vždy zajištěna bezpečnost a přístupy k uloženým heslům byly zabezpečeny na kryptografické úrovni. Ve všech případech musí být vytvářena auditní stopa, která umožní zpětně určit, kdo k jednotlivým heslům přistupoval. Z pohledu přístupu musí řešení podporovat následující typy ukládání hesel

1. Přístup pouze jedné osoby.
2. Přístup více oprávněných osob.
3. Přístup oprávněné osoby nebo přístup na základě kvora (např. tři z pěti osob v roli správce nebo podobné)

### **2. GENEROVÁNÍ HESEL**

Řešení musí mít funkci pro generování náhodných hesel. Tato funkce musí být nastavitelná tak, aby generovala hesla, která jsou v souladu s vyhláškou č. 82/2018 Sb. Řešení musí umožňovat u generovaného i zadávaného hesla zobrazit odhadovanou entropii a musí zajistit možnost kvalitu hesla a případný výskyt duplicit kontrolovat oprávněným pracovníkům bez toho, aby byla ohrožena důvěrnost hesla.

### **3. SPRÁVA UŽIVATELŮ**

Řešení musí umožnit vytváření a správu uživatelů jak interními mechanismy, tak pomocí integrace s Active Directory a to v kombinaci tak, aby bylo možné řešení využívat jak interními tak externími uživateli. Správci řešení musí mít možnost odebrat přístupové oprávnění k uloženým datům.

Řešení musí umožňovat využití dvoufaktorové autentizace a musí být dostupné alespoň pro platformy MS Windows 10, MacOS, iOS a Android.

#### **4. SPRÁVA HESEL LOKÁLNÍCH ADMINISTRÁTORŮ**

Řešení musí umožnit automatizovanou výměnu hesel pro lokální účty koncových stanic a serverů pro systémy MS Windows a MacOS. Výměna hesel musí probíhat v pravidelných intervalech, a to i v případě, že stanice není, v době, kdy má k výměně dojít, připojena k systému. Hesla generovaná pro lokální účty musí být generována tak, aby byla v souladu s vyhláškou č. 82/2018 Sb.

#### **5. INTEGRACE A DALŠÍ FUNKČNÍ POŽADAVKY**

Řešení musí umožňovat hromadný import hesel z formátu CSV a musí umožnit uložení alespoň tisíce hesel pro jednoho uživatele. Řešení musí být implementováno na HW Zadavatele bez potřeby komunikace do cloudu nebo jiných externích systémů.

Veškeré operace s uloženými daty musí být zaznamenány v auditních ložích. Auditní logy pak musí být možné automatizovaně předávat do syslog serveru, aby mohly být nezávisle vyhodnocovány.

Řešení musí umožnit bezpečné zálohování tak, aby při zálohování nemohlo dojít ke kompromitaci dat a zároveň schopnost obnovy řešení tak, aby při obnově byla všechna data a hesla v rámci řešení použitelná. Zde se jedná zejména o generovaná hesla pro lokální administrátory.

#### **6. IMPLEMENTACE**

V rámci této zakázky musí být provedena implementace řešení u Zadavatele. Implementací je míněna instalace řešení, integrace s AD Zadavatele, integrace se Syslog řešením zadavatele a instalace řešení pro správu hesel lokálních administrátorů na 20 vybraných stanic za účasti pracovníků Zadavatele.

Součástí implementace musí být školení správců Zadavatele v sídle Zadavatele, které představí systém, jeho uživatelské rozhraní a jeho správcovské rozhraní. Dále musí školení obsahovat způsob deploymentu řešení pro správu hesel lokálních administrátorů.

Systém musí být implementován centrálně a dostupný pro všechny uživatele přes centrální rozhraní.

#### **7. LICENCE A PODPORA**

Zadavatel požaduje licence minimálně pro 500 uživatelů včetně maintenance pro stejné množství po dobu 36 měsíců. Maintenance je chápána standardní softwarová maintenance, tedy nové verze SW a opravy chyb.

Součástí zakázky je i podpora řešení v celkovém rozsahu 36 MD po dobu 36 měsíců.