Príloha č. 1

Opis predmetu zákazky

1 Predmet zákazky

Názov predmetu zákazky: **Analýza rizík časti informačného systému SIPS ZUC**

2 Opis predmetu zákazky

2.1 **Informácie o informačnom systéme (ďalej len IS) potrebné pre ocenenie prác:**

2.1.1 IS vyvíjaný internými zamestnancami

2.1.2 Architektúra relevantnej časti IS:

* aplikácia (platforma Java, Spring framework)
* web rozhranie pre správu
* komunikačné API rozhranie (vstupno-výstupná komunikácia s inou časťou IS prostredníctvom REST architektúry)
* 1 x rozhranie na externý IS (výstup vybraných dát)
* samostatný databázový server

2.1.3 Používatelia: interní používatelia

2.1.4 Roly: 2 (1 používateľská rola pre správcov systému, 1 rola pre komunikačné API rozhranie)

2.1.5 Niektoré použité bezpečnostné mechanizmy:

* protokol TLS, čipové karty pre používateľov, dvojfaktorová autentifikácia používateľov (vrátane integrácie s AD), elektronický podpis, certifikáty, žurnál s bezpečnostne významnými udalosťami, ochrana údajov (záznamov alebo tabuliek) v databáze

2.2 **Cieľ analýzy rizík IS:**

2.2.1 Cieľom analýzy rizíkIS je vykonať hĺbkovú analýzu rizík týkajúcich sa technického návrhu predmetnej časti IS, vrátane jeho funkčnosti, prevádzky a navrhovaných bezpečnostných mechanizmov.

2.2.2 Úspešný uchádzač vyhotoví požadovanú dokumentáciu v slovenskom, českom alebo anglickom jazyku v písomnej forme a v elektronickej forme na vhodnom médiu vo formátoch aplikačných programov Microsoft Word, Excel, resp. vo formáte PDF.

2.3 **Požiadavky na rozsah prác (časový rozsah max. 3 týždne):**

2.3.1 Výstupom analýzy rizík IS je dokument, ktorý na základe poskytnutých podkladov a dodatočne získaných informácií (prostredníctvom dotazníkov a stretnutí):

* Sumarizuje bezpečnostné požiadavky na systém a navrhované bezpečnostné opatrenia.
* Identifikuje a klasifikuje hrozby relevantné pre túto časť IS.
* Zhodnotí adekvátnosť bezpečnostných požiadaviek a opatrení vzhľadom na identifikované hrozby prostredníctvom hodnotenia rizík IS. Pri hodnotení zohľadní štandardy, odporučenia najlepšej praxe a vlastné skúsenosti. Pri hodnotení rizík IS sa použije škála Critical/High/Medium/Low/Very Low.
* Navrhne úpravy bezpečnostných opatrení alebo nové (dodatočné) opatrenia na naplnenie bezpečnostných požiadaviek, vrátane zhodnotenia dopadov na riziká IS.

2.3.2 Predmetom aktivít uvedených v predchádzajúcom bode sú požiadavky a opatrenia minimálne v nasledujúcich oblastiach:

* Správa systému: funkcie, role a oprávnenia, ochrana komponentov systému a konfigurácie
* Riadenie prístupu: identifikácia a autentifikácia, role a oprávnenia, správa používateľov, riadenie sessions
* Kryptografia: výber, parametre a spôsob použitia kryptografických algoritmov a protokolov, správa a ochrana kryptografických kľúčov (generovanie, distribúcia, uloženie, používanie, výmena, vyradenie a pod.)
* Rozhrania systému: autentifikácia komunikujúcich strán, import a export údajov, zálohovanie a obnova údajov, ochrana údajov (pre jednotlivé rozhrania)
* Údaje uložené v aplikácii: ochrana dôvernosti a integrity údajov
* Audit: vytváranie a rozsah auditných záznamov, ochrana záznamov, vyhodnocovanie
* Dostupnosť systému: redundancia, dostupnosť a riadenie zdrojov.

2.4 **Požiadavky na rozsah prác – voliteľne čerpané konzultačné hodiny (max. 10 hodín):**

2.4.1 Poskytnutie požadovaného počtu konzultačných hodín, po vykonaní analýzy, k hodnoteniu rizík IS a k návrhom bezpečnostných opatrení podľa požiadaviek obstarávateľa.

2.5 **Spôsob realizácie:**

2.5.1 Verejný obstarávateľ poskytne úspešnému uchádzačovi:

* dokumentáciu v slovenskom jazyku: klasifikácia spracovávaných informácií, funkčná špecifikácia IS, relevantné interné predpisy
* dodatočné informácie formou konzultácií s vývojovým tímom a pod .

2.5.2 Úspešný uchádzač vypracuje analýzu bezpečnosti IS vo svojich priestoroch, pričom všetky konzultácie a organizačné náležitosti zákazky vyžadujúce prítomnosť pracovníkov verejného obstarávateľa budú vykonané v priestoroch verejného obstarávateľa.