Załącznik nr 1

**Szczegółowy Opis Przedmiotu Zamówienia**

**Audyt cyberbezpieczeństwa w projekcie Cyfrowa Gmina**

1. **Wytyczne Zamawiającego:**
	1. Audyt musi zostać przeprowadzony zgodnie z załącznikiem nr 8, Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa, który określa wymagania audytu dla projektu Cyfrowa Gmina (Załącznik nr 2 do przedmiotowego postępowania
	- formularz diagnozy).
	2. Działania audytowe realizowane będą w oparciu o:
		* 1. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247, t.j.),
			2. Ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.).
	3. Audyt musi zostać zakończony wykonaniem raportu zawierającego opis wszystkich elementów, które zostały poddane audytowi w podziale na ryzyko (wysoki, średni, niski). Wskazanie zaleceń najlepszych praktyk. Określenie bezpieczeństwa informatycznego w Urzędzie.
2. **Termin wykonania zamówienia:**
	1. Audyt musi zostać wykonany do dnia 20.10.2022 r.
	2. Nie później niż do 27.10.2022 r. wymagane jest przekazanie Zamawiającemu wypełnionego formularza (przeprowadzonej przez osobę posiadająca uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu) przygotowanego zgodnie z wymaganiami programu Cyfrowa Gmina.
	3. Nie później niż do 27.10.2022 r. Wykonawca musi dostarczyć do Zamawiającego dodatkowy dokument przedstawiający wyniki testów i opisujący wszystkie spostrzeżenia oraz zalecenia zmian konfiguracji systemów informatycznych w celu możliwie najlepszego zabezpieczenia sieci oraz urządzeń Zamawiającego.
3. **Odbiór robót:**
	1. Odbiór przez Zamawiającego, nastąpi w ciągu 7 dni od dnia przekazania przez Wykonawcę podpisanego formularza informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa oraz dokumentu przedstawiającego wyniki testów.
	2. Przed podpisaniem protokołu odbioru, osoba pełniąca nadzór nad Zamówieniem po stronie Zamawiającego, ma prawo skontrolować postęp wykonywanych prac.
	3. Podstawę wystawienia faktury, stanowił będzie obustronnie podpisany protokół odbioru.
4. **Audyt cyberbezpieczeństwa może być przeprowadzony wyłącznie przez osoby legitymujące się jednym z poniższych certyfikatów:**
	* 1. Certified Internal Auditor (CIA);
		2. Certified Information System Auditor (CISA);
		3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;
		4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
		5. Certified Information Security Manager (CISM);
		6. Certified in Risk and Information Systems Control (CRISC);
		7. Certified in the Governance of Enterprise IT (CGEIT);
		8. Certified Information Systems Security Professional (CISSP);
		9. Systems Security Certified Practitioner (SSCP);
		10. Certified Reliability Professional;
		11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.
5. **Podstawowe informacje o jednostce, która podlegać będzie audytowi**
6. Typ organizacji: Jednostka Samorządu terytorialnego.
7. Ilość pracowników ~120
8. Lokalizacja: Urząd Miasta Rydułtowy, ul. Ofiar Terroru 36, 44-280 Rydułtowy
9. Liczba serwerów fizycznych: 7
10. Liczba serwerów wirtualnych: 20
11. Liczba stacji roboczych: ~120
12. Liczba urządzeń brzegowych: 5