Załącznik nr 5 do zapytania ofertowego

**Szczegółowy Opis Przedmiotu Zamówienia**

Opis Przedmiotu Zamówienia dotyczącego przeprowadzenia audytu bezpieczeństwa informacji i bezpieczeństwa teleinformatycznego, mającego na celu ocenę poziomu bezpieczeństwa u Zamawiającego (audyt). Audyt powinien objąć wszelkie niezbędne działania w celu określenia stopnia zgodności z przepisami prawa i zaleceniami norm PN-ISO/IEC 27001.

Wynikiem przeprowadzenia audytu będzie opracowany przez wykonawcę, raport zawierający ocenę stanu bezpieczeństwa organizacji. Raport będzie oparty na wynikach przeprowadzonego audytu i wskazywał elementy zgodne z normą i te wymagające poprawy.

Raport będzie zawierał rekomendacje odnośnie koniecznych działań zarówno doraźnych jak i długoterminowych.

## Wymagania:

1. Audyt musi zostać przeprowadzony przez co najmniej dwóch audytorów posiadających doświadczenie poparte przeprowadzeniem co najmniej 8 audytów bezpieczeństwa w okresie ostatnich dwóch lat.

2. Zespół audytowy musi posiadać doświadczenie w zakresie przeprowadzania audytów bezpieczeństwa w przynajmniej trzech różnych profilach organizacji (np. służba zdrowia, produkcja, jednostka samorządowa).

3. Audyt bezpieczeństwa musi zostać przeprowadzony na zgodność z wymaganiami normy ISO PN-EN 27001.

4. Wykonawca przeprowadzi badanie podatności infrastruktury teleinformatycznej zamawiającego, to jest skanowanie podatności. Skanowanie podatności należy przeprowadzić za pomocą narzędzia informatycznego umożliwiającego sprawdzenie oprogramowania w oparciu o wcześniej zdefiniowane przez Wykonawcę słowniki i sygnatury zgodnie z ustaleniami z Zamawiającym. Skanowanie powinno dostarczyć informacje o występujących podatnościach ocenianych zgodnie ze skalą CVSS 3.0 lub CVSS 4.1.

Wykonawca wykona zlecone skanowanie podatności na określonej części infrastruktury systemu. Harmonogram wykonania skanowania podatności musi zostać wcześniej zaakceptowany przez zamawiającego.

Raport przedstawiony przez Wykonawcę z wyników skanowania i identyfikacji podatności musi zawierać informacje o zaistniałych anomaliach w pracy systemu, które zostały odnotowane podczas skanowania podatności i ich krytyczności w odniesieniu do prowadzonej działalności operacyjnej

(usługi kluczowej). Wykonawca dokona priorytetyzacji i klasyfikacji zebranych podatności oraz opracuje sposoby zmniejszenia ryzyka.

5.Wykonawca przeprowadzi badanie zgodności systemów teleinformatycznych zainstalowanych na: serwerach (Windows, Linux), urządzeniach Firewall, Switch oraz baz danych zgodnie z najlepszymi standardami (np. CIS Benchmark, STIG, itp.)

6. Audyt musi być przeprowadzony zgodnie z Planem Audytu (zawierającym harmonogram prac), przygotowanym przez Wykonawcę. Wykonawca do 14 dni po podpisaniu umowy przedstawia Plan Audytu Zamawiającemu celem akceptacji. Zamawiający ma 7 dni od przedstawienia Planu Audytu na jego akceptację lub wniesienie uwag.

7. Plan Audytu musi zawierać następujące elementy: Czynności wykonywane podczas prac audytowych wraz z terminami ich realizacji o Przybliżony termin zakończenia prac audytowych

8. Audyt powinien w zakresie technicznym obejmować następujące elementy:

- techniczne zabezpieczenia stacji roboczych i serwerów,

- techniczne zabezpieczenia infrastruktury sieciowej,

- audyt mechanizmów logowania,

- techniczne zabezpieczenia poczty elektronicznej,

- audyt odporności systemów teleinformatycznych pod kątem cyberzagrożeń.

9. Podczas audytu należy poddać ocenie bezpieczeństwo fizyczne obiektów:

COS-OPO Giżycko, COS-OPO Cetniewo, COS-OPO Wałcz, COS-OPO Spała, COS-OPO Zakopana, COS-OPO Duszniki Zdrój, COS-OPO Szczyrk, COS Warszawa.

10. Podczas audytu należy zbadać bezpieczeństwo sieci bezprzewodowej. Informacje o metodyce badania oraz ocenie i rekomendacjach bezpieczeństwa muszą zostać uwzględnione w raporcie z audytu.

**Wymagania organizacyjne:**

1. Co najmniej dwóch audytorów powinno posiadać:

a) jeden z certyfikatów określonych w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu lub

b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub

c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.

**Wykaz certyfikatów uprawniających do przeprowadzenia audytu:**

I. Certified Internal Auditor (CIA);
II. Certified Information System Auditor (CISA);
III. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN
IV. ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy
V. z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
VI. 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;
VII. Certified Information Security Manager (CISM);
VIII. Certified in Risk and Information Systems Control (CRISC);
IX. Certified in the Governance of Enterprise IT (CGEIT);
X. Certified Information Systems Security Professional (CISSP);
XI. Systems Security Certified Practitioner (SSCP);
XII. Certified Reliability Professional;
XIII. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

**Wymagania dotyczące raportu:**

1. Raport musi zawierać odniesienia do wymagań wynikających z Normy ISO PN-EN 27001.

2. Raport musi uwzględniać opisany stan faktyczny podczas sesji audytowych oraz ocenę i rekomendacje audytowe.

3. Wykonawca zobowiązany jest uwzględnić wszystkie informacje na temat przeprowadzonego audytu technicznego w raporcie z uwzględnieniem zidentyfikowanych podatności oraz proponowane działania naprawcze.