

Załącznik nr 1
do Zapytania ofertowego w celu realizacji zamówienia

OPIS PRZEDMIOTU ZAMÓWIENIA

DOTYCZY:

Usługa polegająca na przeprowadzeniu u Zamawiającego Audytu bezpieczeństwa potwierdzającego zwiększenie poziomu bezpieczeństwa teleinformatycznego.

Zamawiający posiada obecnie aktualne certyfikaty:

- 1) Systemu zarządzania bezpieczeństwem informacji na zgodność z normą PN-ISO/IEC 27001:2017:
Data pierwsze certyfikacji: 5.11.2018
- 2) Systemu zarządzania jakością na zgodność z normą ISO 9001:2015:
Data pierwsze certyfikacji: 28.09.2011

W ramach zawartej umowy Wykonawca:

1. Przeprowadzi Audyt bezpieczeństwa w obu lokalizacjach Zamawiającego (lok. Ligota, Ceglana) w terminie uzgodnionym z Zamawiającym.
2. Audyt bezpieczeństwa poprzedzony będzie audytem wstępnym w siedzibie Zamawiającego w terminie uzgodnionym z Zamawiającym.
3. Audyt przeprowadzony zostanie przez:
 - a) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
 - b) co najmniej dwóch audytorów posiadających:
 - certyfikaty określone w poniższym wykazie certyfikatów uprawniających do przeprowadzenia audytu lub
 - co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
 - 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.
4. Wykaz certyfikatów uprawniających do przeprowadzenia audytu:
 1. Certified Internal Auditor (CIA);
 - 1) Certified Information System Auditor (CISA);
 - 2) 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, w zakresie certyfikacji osób;
 - 3) 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;
 - 4) Certified Information Security Manager (CISM);
 - 5) Certified in Risk and Information Systems Control (CRISC),
 - 6) Certified in the Governance of Enterprise IT (CGEIT);
 - 7) Certified Information Systems Security Professional (CISSP);
 - 8) Systems Security Certified Practitioner (SSCP);
 - 9) Certified Reliability Professional;
 - 10) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

5. Audyt bezpieczeństwa powinien potwierdzić zwiększenie poziomu bezpieczeństwa teleinformatycznego u Zamawiającego po zrealizowaniu zakupów podnoszących poziom Cyberbezpieczeństwa w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości Cyberbezpieczeństwa w formie ankiety.
6. Po Audycie jednostka certyfikująca wyda potwierdzenie/brak potwierdzenia zwiększenia poziomu bezpieczeństwa teleinformatycznego.
7. Minimalny zakres audytu:
 - Weryfikacja pod kątem dojrzałości cybernetycznej w odniesieniu do przeprowadzonego badania poziomu dojrzałości Cyberbezpieczeństwa u Zamawiającego w formie ankiety
 - Ocena urządzeń i konfiguracji pod kątem Cyberbezpieczeństwa (ochrona poczty, sieci, systemów serwerowych, stacji roboczych, systemów bezpieczeństwa)
 - Ocena monitorowania i reakcji na incydenty
 - Ocena zarządzania ciągłością działania
 - Zarządzanie bezpieczeństwem informacji (ocena dokumentacji oraz wdrożonych procedur)
8. Raport z Audytu i wszystkie wynikające z niego zalecenia zostaną udostępnione Zamawiającemu w ciągu 14 dni od zakończenia Audytu.
9. Po zakończeniu Audytu i potwierdzenia zwiększenia poziomu bezpieczeństwa teleinformatycznego jednostka wystawi Zamawiającemu odpowiedni certyfikat
10. Jednostka certyfikująca zachowa poufność wszelkich otrzymanych od Zamawiającego informacji.
11. Zamawiający będzie miał prawo do posługiwania się ważnym certyfikatem oraz znakiem certyfikacji do celów, do których takie certyfikaty są przewidziane i wykorzystywane.
12. Szczegółowo przebieg usługi zostanie określony w Umowie.