Audyt Systemu Bezpieczeństwa Informacji wdrożonego w Urzędzie Gminy w Słońsku wraz z opracowaniem raportu końcowego

Zakres audytu systemu bezpieczeństwa informacji wdrożonego w urzędzie obejmie zgodność z kryteriami zawartymi w § 20 ust. 2 ww. rozporządzenia KRI lub zgodność z wymaganiami normy PN-ISO/IEC 27001, a w szczególności:

1. Analiza Danych i Przepływu Informacji
   - Zrozumienie, jakie dane są przetwarzane, w tym ich wrażliwość i wartość dla organizacji
   - Mapowanie przepływu informacji, aby zidentyfikować, jak dane są udostępniane między dostawcami a użytkownikami końcowymi
2. Identyfikacja Zagrożeń i Ocena Ryzyka
   - Wykrywanie potencjalnych zagrożeń dla systemów IT oraz ocena ryzyka związana z nieautoryzowanym dostępem, wyciekami danych, czy zakłóceniami w świadczeniu usług
   - Ciągłość działania - analiza zdolności organizacji do kontynuowania kluczowych operacji w przypadku cyberataku, w tym plany awaryjne i odtwarzania po awarii
   - Kopie bezpieczeństwa - ocena skuteczności strategii tworzenia kopii zapasowych danych, w tym ich regularności, bezpieczeństwa przechowywania i szybkości odtwarzania
   - Ochrona przed złośliwym oprogramowaniem - analiza skuteczności zastosowanych rozwiązań antywirusowych i antymalware
   - Zarządzanie tożsamościami i dostępem - ocena procedur zarządzania dostępem do systemów i danych, w tym autoryzacji, uwierzytelniania i monitorowania aktywności użytkowników
   - Szyfrowanie danych - ocena stosowania szyfrowania do ochrony danych przechowywanych i przesyłanych, zarówno wewnątrz organizacji, jak i w komunikacji z zewnętrznymi stronami
   - zarządzanie incydentami cyberbezpieczeństwa - ocena planów reagowania na incydenty, w tym procedur zgłaszania, analizy, łagodzenia skutków oraz komunikacji wewnętrznej i zewnętrznej
3. Przegląd Kontroli Bezpieczeństwa
   - Ocena efektywności obecnych mechanizmów bezpieczeństwa i identyfikacja obszarów wymagających poprawy, aby lepiej chronić system przed zagrożeniami
   - Weryfikacja Dokumentacji, Polityk i Procedur

- Sprawdzenie, czy obecna dokumentacja, polityki i procedury bezpieczeństwa są aktualne, adekwatne i zgodne z najlepszymi praktykami oraz wymogami prawnymi

4. Przegląd Mechanizmów Zarządzana i Weryfikacja Zgodności
   - Weryfikacja zgodności z NIS2 – Gap analysis
   - Zarządzanie systemami teleinformatycznymi
   - Zarządzanie incydentami bezpieczeństwa
   - Zarządzanie ciągłością działania
   - Zarządzanie bezpieczeństwem fizycznym organizacji.
5. Tworzenie Profilu Ryzyka i Rekomendacji
   - Użycie zebranych danych do stworzenia kompleksowego profilu ryzyka i opracowanie rekomendacji mających na celu zwiększenie poziomu bezpieczeństwa i zgodności systemów z obowiązującymi standardami.
6. Raport z audytu zostanie podpisany przez audytora dokonującego audyt systemu bezpieczeństwa informacji wdrożonego w Urzędzie Gminy w Słońsku i dostarczony do siedziby JST.
7. Audyt systemu bezpieczeństwa informacji wdrożonego w Urzędzie Gminy w Słońsku zostanie przeprowadzony przez audytora posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999).