ZAŁĄCZNIK NR 1 DO ZAPROSZENIA DO SKŁADANIA OFERT
ZAŁĄCZNIK NR 1 DO UMOWY

OPIS PRZEDMIOTU ZAMÓWIENIA

Przeprowadzenie u Zamawiającego jako operatora usługi kluczowej audytu w zakresie zgodności z ustawą o Krajowym Systemie Cyberbezpieczeństwa z uwzględnieniem dyrektywy NIS2 oraz wdrożenie systemu zarządzania bezpieczeństwem informacji zgodnie z ustawą o Krajowym Systemie Cyberbezpieczeństwa oraz wymaganiami dyrektywy NIS2 w Górnośląskim Przedsiębiorstwie Wodociągów S.A. w Katowicach.

Audyt zgodności z Ustawą o Krajowym Systemie Cyberbezpieczeństwa (UKSC) z uwzględnieniem dyrektywy NIS2

W zakresie dokumentacji dla oceny zgodności z UKSC oraz dyrektywy NIS2 wymagane jest wykonanie sprawdzenia zgodności systemu zarzadzania bezpieczeństwem informacji według kryteriów normy ISO/IEC 27001, oraz dodatkowych kryteriów wskazanych we wspomnianej ustawie wraz z rozporządzeniem.

Audyt musi obejmować aspekty organizacyjne oraz techniczne.

W zakresie organizacyjnym audyt powinien objąć procesy, procedury, politykę wewnętrzną organizacji oraz stosowanie się do zapisów zawartych w dokumentacji jak i w przepisach prawa. Działania audytowe musza obejmować:

- przegląd i analizę polityk bezpieczeństwa organizacji,
- weryfikację zgodności z aktualną Ustawą o UKSC oraz dyrektywą NIS2,
- zarządzanie systemami teleinformatycznymi,
- zarządzanie incydentami bezpieczeństwa,
- zarządzanie ciągłością działania,
- zarządzaniem bezpieczeństwem fizycznym organizacji.

W zakresie technicznym audyt musi obejmować techniczne zabezpieczenia wdrożone w organizacji Zamawiającego.

Działania audytowe musza obejmować:

- techniczne zabezpieczenia serwerów, komputerów oraz stacji roboczych,
- techniczne zabezpieczenia poczty elektronicznej w tym techniczne zabezpieczenia ochrony antywirusowej, antyspamowej,
- techniczne zabezpieczenia infrastruktury sieciowej,

- audyt mechanizmów logowania,
- audyt zarządzania kopiami zapasowymi,
- zarządzanie zmianami w systemach teleinformatycznych,
- audyt weryfikacji i konfiguracji oprogramowania.

W zakresie wymagań NIS2 audytowi muszą być poddane szczegółowo następujące obszary:

- polityka bezpieczeństwa informacji,
- obsługa incydentu,
- ciągłość działania, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej, zarządzanie kryzysowe,
- bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami,
- bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich ujawnianie,
- polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie,
- podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa,
- polityki i procedury stosowania kryptografii i w stosownych przypadkach, szyfrowania,
- bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami,
- w stosownych przypadkach – stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.

Wynikiem audytu powinno być stworzenie raportu zawierającego stwierdzone nieprawidłowości oraz rekomendacje w zakresie rozwiązań zwiększających bezpieczeństwo.

Wymagania prawne stanowiące kryteria audytu:

- Dyrektywa Parlamentu Europejskiego I Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148.
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 1560).

- Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz. U. poz. 1806).
- Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. poz. 2180).
- Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080).
- Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. 2019 poz. 2479).
- Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług (Dz. U. poz. 1830).

Podstawowe wymagania normatywne stanowiące kryteria audytu:

- PN-EN ISO/IEC 27001:2017-06 - „Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania
- ISO/IEC 27001:2022 - Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - System zarządzania bezpieczeństwem informacji - Wymagania
- PN-EN ISO 22301:2020-04 - „Bezpieczeństwo i odporność - Systemy zarządzania ciągłością działania - Wymagania”.

Dodatkowe wymagania normatywne stanowiące pomocnicze kryteria audytu w zakresie bezpieczeństwa fizycznego:

- PN-EN 1627:2021-11 – „Drzwi, okna, ściany osłonowe, kraty i żaluzje - Odporność na włamanie - Wymagania i klasyfikacja”.
- PN-EN 12209:2016-04 – „Okucia budowlane - Zamki mechaniczne wraz z zaczepami - Wymagania i metody badań”.
- PN-EN 50131-1:2009/IS2:2011 – „Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 1: Wymagania systemowe”.

Po wykonanym audycie zostanie przeprowadzone warsztatowe wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji, które polegać będzie na wdrożeniu zaleceń wynikających z audytu i raportu, które zostaną dopasowane do działania organizacji Zamawiającego.

Stworzenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), zgodnie z Normą ISO 27001

Przegląd aktualnej dokumentacji bezpieczeństwa zamawiającego oraz przygotowanie dokumentacji SZBI zgodnie z wymaganiami Normy ISO 27001, ISO 27005.

Główny dokument SZBI, czyli Polityka Bezpieczeństwa Informacji (PBI) musi określać zasady, procedury i wytyczne dotyczące ochrony informacji oraz zapewnienia bezpieczeństwa danych w ramach działalności organizacji i powinna zawierać w szczególności:

- określenie głównych celów polityki oraz zakresu jej stosowania. Wskazanie, jakie informacje są objęte polityką, jakie systemy i procesy są uwzględnione oraz do kogo polityka jest adresowana.
- wytyczne dotyczące bezpiecznego zarządzania informacjami, w tym poufności, integralności, dostępności i autentyczności danych. Zasady te powinny stanowić podstawę postępowania dla pracowników w zakresie ochrony danych.
- określenie ról i odpowiedzialności pracowników w zakresie zapewnienia bezpieczeństwa informacji, włączając w to zarządzanie dostępem, monitorowanie incydentów, audyty bezpieczeństwa, itp.
- wskazówki dotyczące oceny ryzyka, identyfikacji zagrożeń oraz sposobów minimalizowania ryzyka związanego z bezpieczeństwem informacji.
- szczegółowe procedury i wytyczne dotyczące codziennych działań związanych z bezpieczeństwem informacji, takie jak procedury zarządzania hasłami, zarządzanie dostępem, monitorowanie systemów, zarządzanie incydentami, itp.
- określenie procesów audytowych oraz monitorowania systemów, w tym środki kontroli, audyty bezpieczeństwa oraz raportowanie incydentów.
- wskazówki dotyczące szkoleń pracowników w zakresie bezpieczeństwa informacji oraz promowania świadomości bezpieczeństwa w organizacji.

Powyższa dokumentacja powinna być dostosowana do organizacji Zamawiającego. W celu wykonania przedmiotu oferty, SZBI musi być zgodny z procesami realizowanymi przez organizacje oraz zgodny z dyrektywą NIS2. W związku z realizowanymi zadaniami podczas procesu tworzenia dokumentacji, Wykonawca będzie cyklicznie, w zaplanowanym wcześniej okresie, spotykał się z Zamawiającym w celu pozyskiwania niezbędnych informacji do zawarcia w SZBI.

Wymagania dla firm:

Wykonawca ma wdrożony u siebie system zarządzania bezpieczeństwem informacji i musi to potwierdzić posiadanym aktualnym certyfikatem ISO 27001.

Zamawiający nie dopuszcza realizacji części zadań poprzez podwykonawców.