

Znak sprawy: WIN.ZP.271.6.1.2026.MD

OPIS PRZEDMIOTU ZAMÓWIENIA

1. ZAMAWIAJĄCY

Gmina Daleszyce
Pl. Staszica 9
26-021 Daleszyce
NIP: 6572525617,
Regon: 291010040

2. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest **Aktualizacja / opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta i Gminy w Daleszycach oraz 6 jednostkach podległych wraz z przeprowadzeniem szkoleń z zakresu cyberbezpieczeństwa dla pracowników i kadry zarządzającej, w ramach projektu pn. „Cyberbezpieczny Samorząd Gminy Daleszyce”**

Projekt współfinansowany przez Unię Europejską w ramach konkursu grantowego pn. „Cyberbezpieczny Samorząd”, Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach programu FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC)

Zamawiający posiada następujące dokumenty:

a) Urząd Miasta i Gminy w Daleszycach (dalej UMiG):

- Polityka Bezpieczeństwa Informacji
- Instrukcja Zarządzania Systemem Informatycznym
- Analiza poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka

b) Jednostki podległe:

- **Zespół Szkolno-Przedszkolny w Daleszycach (dalej ZSP)**
 - Polityka Ochrony Danych

- Instrukcja Zarządzania Systemem Informatycznym
- Analiza ryzyka przetwarzanych danych pod kątem zapewnienia poufności, integralności i dostępności
- **Miejsko-Gminny Żłobek w Daleszycach (dalej MGŻ)**
 - Polityka Bezpieczeństwa Ochrony Danych Osobowych Miejsko-Gminnego Żłobka w Daleszycach
 - Instrukcja Zarządzania Systemem Informatycznym W Miejsko-Gminnym Żłobku w Daleszycach
- **Szkoła Podstawowa im. Generała Tadeusza Buka w Mójczy (dalej SP w Mójczy)**
 - Polityka Ochrony Danych w Szkole Podstawowej im. Generała Tadeusza Buka w Mójczy
 - Instrukcja Zarządzania Systemem Informatycznym w Szkole Podstawowej im. Generała Tadeusza Buka w Mójczy
 - Analiza Ryzyka i Zagrożeń Przy Przetwarzaniu Danych Osobowych w Szkole Podstawowej im. Generała Tadeusza Buka w Mójczy
- **Szkoła Podstawowa im. Kornela Makuszyńskiego w Niestachowie (dalej SP w Niestachowie)**
 - Instrukcja Zarządzania Systemem Informatycznym w SP Niestachów
 - Polityka Ochrony Danych osobowych w SP Niestachów
 - Analiza Ryzyka i Zagrożeń przy przetwarzaniu danych osobowych w SP Niestachów
- **Szkoła Podstawowa im. Partyzantów Armii Krajowej Ziemi Kieleckiej w Sukowie (dalej SP w Sukowie)**
 - Polityka Ochrony Danych z dnia 27 kwietnia 2024 r.
 - Instrukcja Zarządzenia Systemem Informatycznym z dnia 27 kwietnia 2024r.
 - Analiza ryzyka i zagrożeń przy przetwarzaniu danych osobowych z dnia 3 września 2022 r.
- **Centrum Usług Społecznych w Daleszycach (dalej CUS, dawniej MGOPS)**
 - Polityka Bezpieczeństwa Informacji

Wykonawca w ramach przedmiotu zamówienia:

- 1) będzie świadczyć usługi konsultacyjne, doradcze, analityczne oraz przeprowadzi audyt przedwdrożeniowy celem ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji wg ISO 27001 oraz usług IT w UMiG oraz Jednostkach podległych,
- 2) dokona aktualizacji / opracuje System Zarządzania Bezpieczeństwem Informacji

(SZBI) UMiG oraz Jednostkach podległych, w oparciu o wykonane analizy, Polską Normę PN-ISO/IEC 27001, ustawę o Krajowym Systemie Cyberbezpieczeństwa, dyrektywę NIS2 i Rozporządzenie Parlamentu Europejskiego RODO, ustawę o informatyzacji podmiotów realizujących zadania publiczne oraz inne obowiązujące przepisy w tym zakresie

- 3) kompleksowo przeprowadzi UMiG oraz Jednostki podległe przez proces wdrożenia systemowego podejścia do zarządzania bezpieczeństwem i ciągłością działania, poczynając od ustalenia kontekstu organizacji i celów bezpieczeństwa, przygotuje wymagane normą ISO 27001 dokumenty, a następnie wdroży je do użytku w instytucji,
- 4) wprowadzi zmiany do opracowanych w ramach przedmiotowego zamówienia SZBI, które będą wynikały z przeprowadzonych raportów z audytów,
- 5) przeprowadzi szkolenia dla pracowników oraz kadry zarządzającej UMiG oraz Jednostek podległych z zakresu cyberbezpieczeństwa oraz Systemu Zarządzania Bezpieczeństwem Informacji.

Zamawiający wymaga, aby działania audytowe oraz szkolenia odbywały się stacjonarnie w miejscu i czasie uzgodnionym z Zamawiającym. Wykonawca, w ciągu 14 dni po podpisaniu umowy, opracuje i przedstawi Zamawiającemu szczegółowy harmonogram prac.

Informacje o liczbie pracowników objętych szkoleniem:

- a) Pracownicy Urzędu Miasta i Gminy w Daleszycach – 60 osób,
- b) Kadra zarządzająca UMiG – 12 osób,
- c) Pracownicy Jednostek podległych – 93 osoby.

Uwaga! Liczba pracowników objęta szkoleniem może się różnić od podanej w zapytaniu.

2.1. Etapy realizacji prac i warunki świadczenia usług w zakresie ustanowienia i wdrożenia systemu zarządzania bezpieczeństwem informacji.

- 1) Badanie stanu środowiska UMiG oraz Jednostek podległych pod kątem zgodności z obowiązującymi regulacjami prawnymi przed opracowaniem i wdrożeniem SZBI, w postaci audytów wstępnych mających na celu szczegółową analizę obecnych procesów, procedur operacyjnych oraz mechanizmów kontroli związanych z bezpieczeństwem informacji, w celu zidentyfikowania istniejących luk i obszarów wymagających usprawnienia, wywiad z pracownikami odpowiadającymi za bezpieczeństwo informacji, weryfikacja zgodności dokumentacji oraz procedur

związanych z bezpieczeństwem informacji pod kątem wymagań normy ISO 27001 oraz wymagań KRI i dyrektywy NIS2, analiza luk, opracowanie raportu. Podsumowaniem badania będą:

- a. Raport z audytu dla UMiG
 - b. Raport z audytu dla ZSP
 - c. Raport z audytu dla MGŻ
 - d. Raport z audytu dla SP w Mójczy
 - e. Raport z audytu dla SP w Niestachowie
 - f. Raport z audytu dla SP w Sukowie
 - g. Raport z audytu dla CUS.
- 2) Aktualizacja lub opracowanie i wdrożenie w UMiG oraz Jednostkach podległych „Polityki Bezpieczeństwa Informacji”, w tym analiza kontekstu wewnętrznego i zewnętrznego, ustalenie celów i mierników bezpieczeństwa. Opracowanie materiałów informacyjnych dot. wdrożenia nowej Polityki Bezpieczeństwa Informacji wprowadzającej SZBI, skierowanych do kierownictwa i pracowników.
 - 3) Weryfikacja istniejącej w UMiG oraz Jednostkach podległych „Polityki Ochrony Danych Osobowych” i dostosowanie do opracowywanego SZBI.
 - 4) Wypracowanie dla UMiG oraz Jednostek podległych metodyki zarządzania aktywami informacyjnymi, uwzględniającej cykl życia informacji, przypisanie właścicieli aktywów do realizowanych celów i zadań.
 - 5) Opracowanie i wdrożenie w UMiG oraz Jednostkach podległych mechanizmu identyfikacji i klasyfikacji aktywów oraz Rejestru aktywów zgodnego z ISO 27005. Wykonawca przeprowadzi instruktaż dla kluczowych osób zaangażowanych w identyfikację aktywów, w zakresie sposobu realizacji metodyki.
 - 6) Opracowanie i wdrożenie w UMiG oraz Jednostkach podległych metodyki zarządzania ryzykiem w oparciu o ISO 31000 oraz zdefiniowanie ról i zakresu odpowiedzialności. Przeprowadzenie procesu zarządzania ryzykiem i wdrożenie go w UMiG oraz Jednostkach podległych. Integracja procesu z innymi systemami (np. w zakresie ochrony danych osobowych, kontroli zarządczej), jeśli Zamawiający tak uzna po konsultacjach z Wykonawcą. Przeprowadzenie warsztatów z osobami zaangażowanymi bezpośrednio w proces zarządzania ryzykiem w ramach szkoleń.
 - 7) Wdrożenie w UMiG oraz Jednostkach podległych dokumentacji SZBI wymaganej wg ISO 27001, tj. opracowanie i wdrożenie polityk dziedzinowych, procedur, instrukcji (Instrukcja cyberbezpieczeństwa i Zarządzania Systemami Informatycznymi oraz

Instrukcja reagowania na incydenty).

- 8) Dla UMiG oraz Jednostek podległych, Wykonawca na podstawie wyników uzyskanych w trakcie realizacji badania, o którym mowa w pkt. 1, identyfikacji i klasyfikacji aktywów informacyjnych oraz wyników szacowania ryzyka, przedstawi mapę dokumentów SZBI stanowiącą szczegółowy wykaz dokumentów z określeniem ich wzajemnych powiązań. Na podstawie zatwierdzonej przez UMiG oraz Jednostki podległe propozycji mapy dokumentów SZBI, Wykonawca opracuje wszystkie opisane w koncepcji dokumenty. Dokumenty te muszą być zgodne ze wszystkimi wymaganiami prawnymi. Jeśli w trakcie realizacji umowy wymagania prawne w zakresie bezpieczeństwa informacji ulegną zmianie Wykonawca zobowiązany jest dostosować dokumentację SZBI do zaistniałych zmian. Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanych i przekazanych przez Wykonawcę dokumentów. Wykonawca jest zobowiązany do uwzględnienia w dokumentach uwag wniesionych przez Zamawiającego.

SZBI powinien zawierać w szczególności:

- 1) wzory kart uprawnień oraz zasady nadawania/ odbierania uprawnień,
- 2) instrukcję bezpiecznej eksploatacji systemów i sieci, zasady bezpieczeństwa przy korzystaniu z poczty elektronicznej,
- 3) kopie bezpieczeństwa (analiza i strategia rozwoju),
- 4) zarządzanie i nadzór nad incydentami,
- 5) plan ciągłości działania,
- 6) skróconą dokumentację zawierającą podstawy SZBI niebędących informacją poufną dla pracowników,
- 7) inne dokumenty niż wymienione wyżej, które mogą okazać się niezbędne do zarządzania bezpieczeństwem informacji.

2.2. Warunki świadczenia usług w zakresie szkoleń dla pracowników

Szkolenie dla pracowników oraz kadry zarządzającej UMiG oraz Jednostek podległych ma na celu poszerzenie wiedzy pracowników na temat bezpiecznego korzystania z cyberprzestrzeni w miejscu pracy i poza nim co najmniej w zakresie:

- 1) czym jest cyberbezpieczeństwo,

- 2) omówienie poprawnych zasad związanych z cyberbezpieczeństwem w Urzędzie,
- 3) jak definiować i charakteryzować najważniejsze techniki cyberataków,
- 4) jak rozpoznawać i zapobiegać zagrożeniom związanym z cyberprzestrzenią,
- 5) jak podejmować odpowiednia działania w przypadku cyberataku,
- 6) jak stosować odpowiednie zabezpieczenia utrudniające przeprowadzenie cyberataku,
- 7) jak rozpoznawać socjotechniki wykorzystywane przez cyberprzestępców.
- 8) szczegółowe omówienie zagrożeń w sieci takich jak phishing, ransomware, malware, socjotechnika, atak telefoniczny, spoofing, atak odwrócony - zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa, fałszywe wiadomości mailowych, SMS wraz z przykładami i wskazaniem sposobów przeciwdziałania oraz zabezpieczania się przed powyższymi zagrożeniami,
- 9) metody nieautoryzowanego pozyskania danych wraz z przykładami
- 10) bezpieczne przetwarzanie danych: szyfrowanie, przechowywanie, udostępnianie, komunikacja
- 11) bezpieczne hasła, menedżer haseł, autoryzacja dwuetapowa, klucze sprzętowe
- 12) metody obrony oraz przeciwdziałania (w tym: przed wyłudzeniem danych osobowych za pomocą metod socjotechnicznych, programowaniem mogącym zablokować dostęp do urządzeń urzędu, szkodliwymi programami mogącymi pozyskać dane firmowe lub osobiste
- 13) bezpieczne korzystanie z mediów społecznościowych
- 14) bezpieczne korzystanie ze smartfonów
- 15) wskazanie miejsc organizacji oraz informacji, które należy chronić, by zniwelować ryzyko narażenia firmy na straty finansowe,
- 16) stosowania wdrożonych polityk SZBI i procedur

2.2.1. Organizacja szkolenia

- 1) Szkolenie należy przeprowadzić z uwzględnieniem faktu, że uczestnicy szkolenia mogą nie posiadać wiedzy informatycznej i technicznej,
- 2) Miejsce szkolenia oraz ilość grup szkoleniowych należy uzgodnić z Zamawiającym.
- 3) Czas trwania szkolenia dla pojedynczej grupy szkoleniowej – co najmniej 4 godziny zegarowe.
- 4) Wykonawca w ramach wykonania usługi przygotowuje harmonogram szkolenia oraz

program szkolenia i dostarczy je w terminie nie później niż 7 dni roboczych przed dniem rozpoczęcia szkolenia do akceptacji Zamawiającego.

- 5) Harmonogram powinien obejmować informacje dotyczące tematyki i czasu szkolenia
- 6) Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika, pozwalające na samodzielną edukację z zakresu tematyki szkolenia.
- 7) Zamawiający dopuszcza dostarczenie każdemu użytkownikowi kompletu materiałów w formie elektronicznej, np. dokumenty w standardzie PDF
- 8) Wykonawca dostarczy materiały szkoleniowe uczestnikom szkolenia najpóźniej w dniu rozpoczęcia szkolenia
- 9) Wykonawca przygotuje Zamawiającemu materiały ze szkolenia, które to będzie mógł wykorzystać do przeszkolenia osób nieobecnych lub nowo przyjętych.
- 10) Wszelkie koszty opracowania materiałów szkoleniowych ponosi Wykonawca
- 11) Wykonawca nie jest zobowiązany do zapewnienia uczestnikom wyżywienia
- 12) Wykonawca umożliwi uczestnikom skorzystać z konsultacji po ukończeniu szkolenia
- 13) Wykonawca w ramach wynagrodzenia zapewni uczestnikom szkolenia imienne certyfikaty potwierdzające ukończenie szkolenia i jego zakres.

3. WARUNKI ŚWIADCZENIA USŁUG W ZAKRESIE SZKOLEŃ DLA KADRY ZARZĄDZAJĄCEJ UMiG

- 1) Szkolenie ma na celu poszerzenie wiedzy kadry zarządzającej na temat bezpiecznego korzystania z cyberprzestrzeni w miejscu pracy i poza nim co najmniej w zakresie tożsamym z szkoleniami pracowników.
- 2) Szkolenie musi obejmować tematy związane ze stosowaniem wdrożonych polityk SZBI i procedur, przez kadrę zarządzającą oraz obowiązki wynikające z aktualnych przepisów prawa.
- 3) Wykonawca w ramach wynagrodzenia zapewni uczestnikom szkolenia imienne certyfikaty potwierdzające ukończenie szkolenia i jego zakres.