2025-205350

Załącznik nr 1 do Zapytania

OPIS PRZEDMIOTU ZAMÓWIENIA

I. Przedmiot zamówienia

Przedmiotem zamówienia jest **przeprowadzenie audytu dojrzałości oraz aktualizacja i opracowanie nowych procedur CSIRT CeZ**, mających na celu podniesienie skuteczności reagowania na incydenty cyberbezpieczeństwa w sektorze ochrony zdrowia.

II. Definicje

CSIRT CeZ – zespół reagowania na incydenty bezpieczeństwa komputerowego funkcjonujący w strukturze Centrum eZdrowia.

Audyt dojrzałości – usługa oceny poziomu dojrzałości procesów, organizacji i narzędzi CSIRT przy użyciu modelu SIM3 w najnowszej wersji obowiązującej na dzień publikacji ogłoszenia.

Procedury operacyjne (SOP) – zestaw wewnętrznych, wersjonowanych dokumentów regulujących standardowe postępowanie CSIRT w procesie zarządzania incydentami.

Model SIM3 – Security Incident Management Maturity Model, model referencyjny oceny dojrzałości CSIRT zalecany przez ENISA w najnowszej wersji obowiązującej na dzień publikacji ogłoszenia.

KSC – ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2023 r., poz. 913 z późn. zm.).

RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Zamawiający – Centrum eZdrowia.

Wykonawca – podmiot wybrany do realizacji niniejszego zamówienia.

OPZ – niniejszy Opis Przedmiotu Zamówienia.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

III. Cel zamówienia

Kompleksowa ocena aktualnego poziomu dojrzałości CSIRT CeZ w aspekcie organizacyjnym i technicznym zgodnie z framework SIM3 w najnowszej wersji obowiązującej na dzień składania ofert.

Aktualizacja istniejących oraz opracowanie nowych procesów i procedur w zakresie reagowania na incydenty cyberbezpieczeństwa oraz w zgodności z framework SIM3 w najnowszej wersji obowiązującej na dzień składania ofert.

Podniesienie skuteczności i efektywności działań CSIRT CeZ poprzez wdrożenie usprawnionych rozwiązań proceduralnych w zgodności z framework SIM3 w najnowszej wersji obowiązującej na dzień składania ofert.

Zapewnienie zgodności procedur CSIRT CeZ z:

1. KSC
2. RODO
3. Normami:

3.1. ISO/IEC:27001

3.2. ISO/IEC:27035

3.3. ISO/IEC:22301

IV. Termin i sposób realizacji zamówienia

Łączny termin realizacji zamówienia: 90 dni kalendarzowych od daty podpisania umowy.

Etap I – Audyt dojrzałości CSIRT CeZ: do 30 dni.

Etap II – Opracowanie dokumentacji proceduralnej (wraz z Etapem I): do 60 dni łącznie.

Rezultatem prac, poza kompletem procedur, będzie również opracowanie zestawu wytycznych i zaleceń umożliwiających przygotowanie CSIRT CeZ do certyfikacji Trusted Introducer zgodnie z modelem dojrzałości SIM3 w najnowszej wersji obowiązującej na dzień publikacji ogłoszenia.

Etap III - Konsultacje i odbiór dokumentacji: do 30 dni.

Zadania realizowane będą w siedzibie Zamawiającego w Warszawie lub zdalnie, w zależności od charakteru czynności.

V. Zakres przedmiotu zamówienia

Etap I – Audyt dojrzałości CSIRT CeZ

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

Przegląd aktualnego stanu funkcjonowania CSIRT CeZ w zakresie:

1. Struktury organizacyjnej;
2. Ról i odpowiedzialności;
3. Procedur operacyjnych;
4. Wykorzystywanych narzędzi i systemów;
5. Procesów zarządzania incydentami;
6. Wymiany informacji i współpracy z innymi podmiotami, w szczególności:

..6.1. CSIRT NASK

..6.2. CSIRT GOV

Analiza dokumentacji istniejących procedur oraz ich zgodności z:

1. Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
2. RODO;
3. Serią norm ISO/IEC 27035.

Warsztaty i wywiady indywidualne z pracownikami CSIRT CeZ.

Ocena dojrzałości przy użyciu modelu SIM3 w najnowszej wersji obowiązującej na dzień publikacji ogłoszenia.

Opracowanie raportu z audytu zawierającego m.in.

1. Ocenę obszarów;
2. Identyfikację luk;
3. Zalecenia rozwojowe;
4. Rekomendacje zmian proceduralnych oraz narzędziowych.

Etap II – Opracowanie dokumentacji proceduralnej

Aktualizacja istniejących dokumentów normatywnych i proceduralnych z uwzględnieniem wyników audytu.

Opracowanie nowych procedur w następujących obszarach:

1. Klasyfikacja i priorytetyzacja incydentów
2. Eskalacja i komunikacja wewnętrzna/zewnętrzna
3. Zarządzanie incydentami technicznymi i organizacyjnymi

Współpraca z zewnętrznymi CSIRT-ami

4. Dokumentowanie i raportowanie incydentów
5. Analiza przyczyn pierwotnych (root cause analysis)

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

6. Postępowanie po incydencie (lessons learned)

7. Zarządzanie incydentami z naruszeniem danych osobowych

8. Audyty i przeglądy w obszarze CSIRT

Dokumentacja musi uwzględniać:

1. Normy

..1.1. ISO/IEC 27001

..1.2. ISO/IEC 27035

..1.3. ISO/IEC 22301

2. Wytyczne ENISA

3. RFC 2350

4. Przepisy ustawy o o krajowym systemie cyberbezpieczeństwa

Etap III – Konsultacje i odbiór dokumentacji

Spotkanie przeglądowe z Zamawiającym.

1. Uwzględnienie uwag i wprowadzenie zmian.

2. Przekazanie dokumentacji w formatach edytowalnych z wersjonowaniem i metryczką zmian:

..2.1. .docx lub .odt

..2.2. PDF

VI. Wymagania wobec Wykonawcy

Realizacja min. dwóch zleceń w ciągu ostatnich pięciu lat dotyczących przeprowadzenia audytu CSIRT/SOC lub opracowania dokumentacji proceduralnej w obszarze CSIRT/SOC.

Zespół wykonawczy obejmuje co najmniej:

1. Eksperta ds. cyberbezpieczeństwa z certyfikacją określoną w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018.1999 z dnia 2018.10.18) - w szczególności: CISSP/CISM/CISA,

2. Specjalistę z certyfikacją Certified SIM3 Auditor oraz udokumentowanym doświadczeniem w pracy z modelem SIM3 – minimum 3 lata.

Wykonawca zobowiązuje się do zachowania poufności i przestrzegania wymogów RODO.

VII. Produkty końcowe i sposób odbioru

Raport z audytu dojrzałości CSIRT CeZ.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

Zestaw procedur operacyjnych CSIRT CeZ.

Dokument podsumowujący rekomendacje strategiczne.

Odbiór etapowy zgodnie z harmonogramem - każdy dokument podlega akceptacji Zamawiającego.

VIII. Wymogi formalne

Wszystkie dokumenty opracowane w języku polskim.

Dokumentacja powinna spełniać następujące kryteria:

8.2.1 odpowiadać wymaganiom modelu SIM3 na poziomie co najmniej TI Certified,

8.2.2 zachowywać spójność w zakresie terminologii, struktury oraz układu treści,

8.2.3 zawierać jednoznaczne i precyzyjne sformułowania, umożliwiające jej prawidłowe zastosowanie w praktyce,

8.2.4 być opracowana w sposób przejrzysty, z zachowaniem podziału na rozdziały, podrozdziały, tabele i/lub schematy tam, gdzie to uzasadnione,

Ostateczna wersja dokumentacji musi zostać zatwierdzona przez Zamawiającego.

IX. Poufność i ochrona danych

Wykonawca zobowiązuje się do zachowania poufności wszelkich informacji uzyskanych w trakcie realizacji zamówienia oraz do przestrzegania przepisów RODO.

X. Postanowienia końcowe

Wszelkie zmiany w zakresie zamówienia wymagają formy pisemnej.

W kwestiach nieuregulowanych OPZ zastosowanie mają przepisy Kodeksu cywilnego oraz Ustawy Prawo zamówień publicznych.

OPZ stanowi integralną część umowy zawieranej z Wykonawcą.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706