



Cyberbezpieczny Samorząd

Zamówienie finansowane ze środków FUNDUSZY EUROPEJSKICH NA ROZWÓJ CYFROWY 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Poprawa bezpieczeństwa – obszar organizacyjny

Zadanie nr 1. Audyt wstępny i konsultacje określające poziom cyberbezpieczeństwa zamawiającego przed wdrożeniem SZBI.

Przeprowadzenie audytu wstępnego i konsultacji określających poziom cyberbezpieczeństwa przed wdrożeniem Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) obejmującego weryfikację zgodności przyjętych procedur z przepisami:

-Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych:

- z zakresu cyberbezpieczeństwa w oparciu o przepisy Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r.poz. 913, 1703);

- z zakresu ochrony danych w oparciu o przepisy Rozporządzenia 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) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

- Ustawie o Krajowym Systemie Cyberbezpieczeństwa, która dodatkowo wskazuje na standardy i obowiązki związane z bezpieczeństwem informacjiKrajowy system cyberbezpieczeństwa (Dz.U.2024.1077).

- Międzynarodowej normie PN-EN ISO/IEC 27001:2023 jako najlepszej praktyce wdrażania SZBI,

- Międzynarodowej normie PN-EN ISO 22301 dotyczącej zarządzania ciągłością działania, rekomendowanej przy wdrażaniu SZCD.

Usługa w terminie do 30 dni kalendarzowych od dnia zawarcia umowy

Zadanie nr 2. Opracowanie dokumentacji SZBI

Przygotowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) składającego się z :

- Polityki Bezpieczeństwa Informacji,

- Polityki Zarządzania Systemem Teleinformatycznym,

- Polityki Zarządzania Ciągłością Działania wraz z Planami Ciągłości Działania oraz analizą BIA,

- Polityki Zarządzania Incydentami Cyberbezpieczeństwa;

- Polityki Ochrony Danych wraz z procedurami wynikającymi z przepisów RODO oraz dobrych praktyk;



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- Analizy Ryzyka Bezpieczeństwa Informacji w obszarze IT

oraz zostaną wprowadzone/dostosowane procedury:

- procedury korzystania z urządzeń mobilnych,
- procedury pracy zdalnej,
- postępowanie z nośnikami,
- procedury kontroli dostępu,
- zabezpieczenie pomieszczeń i obiektów,
- procedury czystego biurka,
- procedury czystego ekranu,
- procedury kopii zapasowych,
- procedury ochrony logów,
- bezpieczeństwo komunikacji,
- zarządzanie bezpieczeństwem sieci,
- przesyłanie informacji,
- plany ciągłości działania,
- procedury zarządzania incydentami,
- prywatność i ochrona danych osobowych,
- szacowanie ryzyka w obszarze bezpieczeństwa informacji,
- szkolenia personelu,
- plan zarządzania podatnościami,
- plan reagowania na incydenty,
- plan przywracania,
- Analiza ryzyka i aktualizacja polityk i procedur w okresie do końca czerwca 2026r.

Wyżej wymieniona dokumentacja musi mieć zgodności z przepisami:

- Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
- z zakresu cyberbezpieczeństwa w oparciu o przepisy Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r.poz. 913, 1703);
- z zakresu ochrony danych w oparciu o przepisy Rozporządzenia 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) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
- Ustawie o Krajowym Systemie Cyberbezpieczeństwa, która dodatkowo wskazuje na standardy i obowiązki związane z bezpieczeństwem informacji. Krajowy system cyberbezpieczeństwa (Dz.U.2024.1077).
- Międzynarodowej normie PN-EN ISO/IEC 27001:2023 jako najlepszej praktyce wdrażania SZBI,
- Międzynarodowej normie PN-EN ISO 22301 dotyczącej zarządzania ciągłością działania, rekomendowanej przy wdrażaniu SZCD.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

Dokumentacja musi zostać zatwierdzona przez Inspektora Ochrony Danych Zamawiającego

Zamawiający otrzyma wyżej wymienioną dokumentację SZBI w wersji elektronicznej-edytowalnej oraz w wersji papierowej.

Usługa w terminie do 90 dni kalendarzowych od dnia zawarcia umowy

Zadanie nr 3. Usługi w zakresie utrzymania dokumentacji SZBI i pełnienia funkcji koordynatora ds. Krajowego Systemu Cyberbezpieczeństwa.

Doradztwo w zakresie ustawy o Krajowym Systemie Cyberbezpieczeństwa - outsourcing usług związanych z pełnieniem funkcji Koordynatora ds. KSC.

Zakres doradztwa:

- 1) Opracowanie procedury, w tym dokumentacji dotyczącej reagowania na incydenty
- 2) Pełnienie funkcji osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz wykonywania wobec tych podmiotów obowiązków
- 3) Świadczenie pomocy w przygotowywaniu zgłoszeń do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego – CDIRT
- 4) Doradztwo w zakresie przekazanych zaleceń pokontrolnych dotyczących usunięcia stwierdzonych nieprawidłowości, wydanych w protokole kontroli przez organ właściwy do spraw cyberbezpieczeństwa
- 5) Przygotowywanie projektów informacji do organu właściwego do spraw cyberbezpieczeństwa o sposobie wykonania zaleceń
- 6) Sporządzenie informacji dotyczących prawnych zagadnień bezpieczeństwa informacji oraz cyberbezpieczeństwa
- 7) Doradztwo w zarządzaniu incydentami oraz doradztwo w obsłudze incydentów
- 8) Opracowanie i aktualizacja broszury pozwalającej na zrozumienie zagrożenia w obszarze cyberbezpieczeństwa i stosowania praktycznych sposobów zabezpieczania się przed tymi zagrożeniami w związku z realizacją zadań publicznych z wykorzystaniem systemów informacyjnych.

Usługa do realizacji do 30 czerwca 2026 od zawarcia umowy.

Zadanie nr 4. Audyt wdrożonego SZBI.

Audyt końcowy wdrożonego SZBI wraz z Audytem Bezpieczeństwa Informacji zgodnym z przepisami Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t. j. Dz. U. 2024 r., poz. 773) wraz z **Ankieta końcowa - Ankieta Dojrzałości cyberbezpieczeństwa wg załącznika Nr 6 do regulaminu konkursu grantowego „Cyberbezpieczny Samorząd”.**

Usługa w terminie do 120 dni kalendarzowych od dnia zawarcia umowy (nie później niż do 30 czerwca 2026 r.)



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA