

PRZEDMIOT ZAMÓWIENIA

1. System zarządzanie bezpieczeństwem informacji (SZBI)

Wdrożenie/aktualizacja wraz z przekazaniem praw autorskich dokumentacji SZBI zgodnie z wymaganiami PN-EN ISO/IEC 27001:2023, ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2024.307 lub nowszą), 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 (Dz.U.2024 poz.773), oraz ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz.U.2024 poz.1077)

Przeprowadzenia szkolenia z wdrożonego systemu SZBI.

2. Polityka Bezpieczeństwa Informacji (PBI)

Opracowanie/aktualizacja Polityki Bezpieczeństwa Informacji w ramach dokumentacji SZBI, która uwzględni kontekst JST, realizowane procesy, strukturę organizacyjną, infrastrukturę, systemy informatyczne JST.

3. Audyt KRI – 2 szt.

Wykonanie audytu zgodnie z wymaganiami art. 21 - 23 ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) i § 19 rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI) w szczególności:

1. Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)

- a) wyznaczenie osoby do kontaktu – KSC
- b) przekazanie danych osoby wyznaczonej – KSC
- c) zapewnienie zarządzania incydem – KSC
- d) zgłaszanie incydemu – KSC
- e) zapewnienie obsługi incydemu – KSC
- f) zapewnienie dostępu do wiedzy – KSC
- g) opracowanie, ustanowienie i wdrożenie SZBI – KRI
- h) monitorowanie i przegląd SZBI – KRI
- i) doskonalenie SZBI – KRI
- j) aktualizowanie regulacji wewnętrznych – KRI
- k) inwentaryzacja sprzętu i oprogramowania – KRI
- l) przeprowadzanie okresowych analiz ryzyka – KRI
- m) postępowanie z ryzykiem – KRI
- n) zarządzanie uprawnieniami – KRI
- o) szkolenia i uświadamianie – KRI
- p) monitorowanie dostępu do informacji – KRI
- q) monitorowanie nieautoryzowanych zmian – KRI

- r) zabezpieczenie nieautoryzowanego dostępu – KRI
- s) ustanowienie zasad bezpiecznej pracy mobilnej – KRI
- t) zabezpieczenie informacji przed nieuprawnionym ujawnieniem – KRI
- u) zabezpieczenie informacji przed nieuprawnioną modyfikacją – KRI
- v) zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem – KRI
- w) zawieranie w umowach serwisowych zapisów o bezpieczeństwie – KRI
- x) ustalenie zasad postępowania z informacjami w celu minimalizacji kradzieży informacji i środków przetwarzania – KRI
- y) aktualizowanie oprogramowania – KRI
- z) minimalizowanie ryzyka utraty informacji w wyniku awarii systemu – KRI
- aa) ochrona systemu przed błędami – KRI
- bb) stosowanie mechanizmów kryptograficznych w systemach – KRI
- cc) zapewnienie bezpieczeństwa plików systemowych – KRI
- dd) zarządzanie podatnościami systemów – KRI
- ee) kontrola zgodności systemów z regulacjami – KRI
- ff) zapewnienie audytu bezpieczeństwa informacji nie rzadziej niż raz na rok – KRI

2. Opracowanie raportu z audytu wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych i korygujących. Audyt systemu bezpieczeństwa informacji wdrożonego w urzędzie JST obejmie zgodność z kryteriami zawartymi w § 19 ust. 2 ww. rozporządzenia KRI lub zgodność z wymaganiami normy PN-EN ISO/IEC 27001:2023. Dodatkowo audyt musi spełniać wymagania Regulaminu Konkursu Grantowego pn. „Cyberbezpieczny Samorząd” Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.

Pierwszy audyt należy wykonać za rok 2024 w terminie do 30.04.2025 r.

Drugi audyt na zakończenie projektu „Cyberbezpieczny Samorząd” przez Zamawiającego jednak nie później niż do 30.06.2026 r.

Wymaganie dla audytora:

1. Audytor posiada 2 letnie doświadczenie w przeprowadzaniu audytów bezpieczeństwa, w tym przeprowadził minimum 2 audyty, które obejmowały zgodność z kryteriami zawartymi w § 20 ust. 2 lub § 19 ust. 2 rozporządzenia Rady Ministrów z dnia odpowiednio 12 kwietnia 2012 r. lub 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.
2. W okresie ostatnich dwóch lat licząc wstecz od dnia, w którym upływa termin składania ofert opracował i wdrożył co najmniej jeden system zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

3. Posiada minimum dwuletnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość o zagrożeniach cybernetycznych.