*Załącznik nr 1 do Zapytania Ofertowego*

**OPIS PRZEDMIOTU ZAMÓWIENIA**

w postępowaniu o udzielenie zamówienia publicznego w trybie Zapytania Ofertowego, pod nazwą:

**Opracowanie dokumentacji SZBI**

realizowanego w ramach projektu

**„Cyberbezpieczny Samorząd Gmina Rabka Zdrój”**

**Zamawiający**: Gmina Rabka Zdrój, ul Parkowa 2, 34-700 Rabka Zdrój

Projekt finansowany ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II „Zaawansowane usługi cyfrowe” Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa”

**Podstawy Prawne**

[Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW](http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.POL&toc=OJ:L:2016:119:TOC).

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).

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.

Rozporządzenie 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.

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 (dyrektywa NIS 2).

Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi.

Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 2 listopada 2006 r. w sprawie wymagań technicznych formatów zapisu i informatycznych nośników danych, na których utrwalono materiały archiwalne przekazywane do archiwów państwowych.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Ustawa z dnia 5 września 2016 o usługach zaufania oraz identyfikacji elektronicznej.

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Narodowe Standardy Cyberbezpieczeństwa

**Zgodność z normami**

Dokumentacja musi być zgodna z aktualnymi na czas realizacji normami:

PN ISO/IEC 27001:2023 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Systemy zarządzania bezpieczeństwem informacji – Wymagania

ISO/IEC 27701:2019 Techniki bezpieczeństwa - rozszerzenie do ISO / IEC 27001 i ISO / IEC 27002

dla zarządzania informacjami o prywatności - wymagania i wytyczne

PN ISO/IEC 27002:2022 Praktyczne zasady zabezpieczania informacji

PN ISO/IEC 27005:2022 Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji

PN-EN ISO 22301 Bezpieczeństwo powszechne -- Systemy zarządzania ciągłością działania -- Wymagania.

PN-ISO/IEC 20000-1 Technika informatyczna. Zarządzanie usługami. Część 1: Wymagania dla systemu zarządzania

PN ISO/IEC 27000 Systemy zarządzania bezpieczeństwem informacji -- Przegląd i terminologia

PN-ISO/IEC 27013 Wytyczne do zintegrowanego wdrożenia ISO/IEC 27001 oraz ISO/IEC 20000-1

PN-EN ISO /IEC 27018 Praktyczne zasady ochrony danych identyfikujących OSOBĘ (PII) w chmurach publicznych działających jako przetwarzający PII

PN-EN ISO /IEC 2737 Wytyczne dotyczące identyfikowania, gromadzenia i przechowywania cyfrowego materiału dowodowego

PN-EN ISO /IEC 2738 Specyfikacja metod cyfrowych trwałego usuwania

PN – ISO 31000 Zarzadzanie ryzykiem zasady i wytyczne

PN-ISO/IEC 20000-2 Technika informatyczna. Zarządzanie usługami. Część 2: Reguły postępowania

PN-EN ISO/IEC 27040 Techniki bezpieczeństwa – Bezpieczeństwo pamięci masowych

PN-EN ISO/IEC 27041 Wytyczne do zapewnienia stosowności i adekwatności metody dochodzeniowej w związku z incydentem

PN-EN ISO/IEC 27042 Wytyczne do analizy i interpretacji cyfrowego śladu dowodowego

PN-EN ISO/IEC 27043 Pryncypia i procesy w dochodzeniach związanych z incydentami

PN-EN ISO /IEC 24762 Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie

**Zakres opracowania dokumentacji SZBI**

1. Zamawiający wymaga opracowania dokumentacji SZBI dla niżej wymienionych podmiotów JST:
2. Urząd Miejski w Rabce Zdroju
3. Szkoła Podstawowa Nr 1 w Rabce-Zdroju
4. Szkoła Podstawowa Nr 2 w Rabce-Zdroju
5. Szkoła Podstawowa Nr 3 w Rabce-Zdroju
6. Szkoła Podstawowa Nr 4 w Rabce-Zdroju
7. Szkoła Podstawowa w Chabówce
8. Szkoła Podstawowa w Ponicach
9. Szkoła Podstawowa w Rdzawce
10. Miejska Biblioteka Publiczna
11. Centrum Kultury, Sportu i Promocji w Rabce-Zdroju
12. Ośrodek Pomocy Społecznej w Rabce-Zdrój
13. Zakład Gospodarki Mieszkaniowej w Rabce-Zdroju
14. Przedszkole nr 1 w Rabce-Zdroju
15. Przedszkole w Chabówce
16. Zespół Przedszkoli Specjalnych w Rabce-Zdroju
17. Dokumentacji musi obejmować opracowanie wymagań dokumentacyjnych systemu SZBI zgodnie z zasadą HLS z zastosowaniem aktualnych norm ISO 27001, ISO 22301, ISO 20000-1 dla wspólnego opisu procesów, przeznaczonych do dalszego wdrożenia dla wskazanych 4 obszarów funkcjonowania Zamawiającego w kontekście wymagań normatywnych aktualnej normy PN-ISO/IEC 27001:2023 dla systemu dokumentacyjnego i obowiązujących normatywne zabezpieczeń jako wypełnienie obowiązków wynikających z Krajowych Ram Interoperacyjności i Ustawy o Krajowym Systemie Cyberbezpieczeńtwa tj.:
18. Obszar 1: Zabezpieczenia organizacyjne
19. Obszar 2: Zabezpieczenia zasobów ludzkich
20. Obszar 3: Zabezpieczenia fizyczne
21. Obszar 4: Zabezpieczenia technologiczne
22. Dokumentacji musi obejmować w szczególności:
23. przeprowadzenie audytu istniejącej dokumentacji SZBI oraz przeprowadzić aktualizację uwzględniającą nowe wydanie normy ISO27001 oraz nowe rozwiązania z zakresu cyberbezpieczeństwa, wdrożone w ramach realizacji projektu pn.: „Cyberbezpieczny Samorząd”;
24. określenie i sformalizowanie zasad zarządzania w szczególności poprzez wskazanie ról dla osób odpowiedzialnych oraz wskazanie podejścia do zapewnienia zasobów niezbędnych do efektywnego zarządzania bezpieczeństwem i zarządzania usługami;
25. określenie i sformalizowanie procedury przeprowadzania audytów bezpieczeństwa , zawierających wskazanie częstotliwości audytów, sposobu przygotowywania i zatwierdzania ich planów, sposobu ich przeprowadzania oraz dokumentowania i raportowania ich wyników;
26. określenie i sformalizowanie procedury działań korygujących w przypadku niezgodności z wymaganiami systemu zarządzania bezpieczeństwem informacji z elementami ciągłości działania;
27. określenie i sformalizowanie procedury wprowadzania działań zapobiegawczych w przypadku wystąpienia sytuacji mogącej prowadzić do niezgodności z wymaganiami systemu zarządzania bezpieczeństwem informacji;
28. określenie i sformalizowanie procedury przeglądu systemu zarządzania bezpieczeństwem informacji w szczególności określającej częstotliwość przeglądów, zakres i sposób ich przeprowadzania, materiały źródłowe niezbędne do przeprowadzenia przeglądu, tryb wdrażania wniosków;
29. określenie i sformalizowanie procedury nadzoru nad dokumentami wchodzącymi w skład systemu zarządzania bezpieczeństwem informacji;
30. określenie i sformalizowanie procedury nadzoru nad zapisami, określającej zasady/zapisy/wymagania przechowywania, archiwizowania oraz niszczenia zapisów;
31. opracowanie nowych procedur zarządzania ryzykiem uwzględniających nowe rozwiązania cyberbezpieczeństwa, a w tym procedury analizy ryzyka, planu zarządzania zagrożeniami i podatnościami, przeprowadzenie oceny ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych przez organizację zgodnie z wytycznymi aktualnej normy PNISO/IEC 27005 wraz z przygotowaniem planu postępowania z ryzykiem zawierający m.in.:
32. zdefiniowanie sposobu pomiaru ryzyka w oparciu o rekomendacje aktualnej normy PN-ISO/IEC 27005;
33. zdefiniowanie i opisanie procesu zarządzania ryzykiem;
34. zdefiniowanie i opisanie inwentaryzacji aktywów informacyjnych lub grup aktywów informacyjnych zgodnie z normą PN-ISO/IEC 27005;
35. zdefiniowanie i opisanie katalogu zagrożeń i oszacowanie prawdopodobieństw ich występowania
36. zdefiniowanie i opisanie identyfikacji ryzyka, szacowanie ryzyk, rejestr ryzyk;
37. zdefiniowanie i opisanie planu reagowania na zagrożenia z uwzględnieniem nowego wydania normy ISO27001 oraz nowych rozwiązań cyberbezpieczeństwa.
38. W ramach określenia i opisu zabezpieczeń dla wymagań systemu bezpieczeństwa informacji zostaną opracowane formalne dokumenty, możliwym wykorzystaniem opisów zawartych w PN EN/ISO IEC 27002:2022 , Narodowych Standardach Cyberbezpieczeństwa jako z źródło tzw. stosowanych praktyk dla opracowywanych dokumentów jako zasady/zapisy/wymagania dla :
39. Obszaru 1: Zabezpieczenia organizacyjne

* polityka bezpieczeństwa informacji
* role i obowiązki w zakresie bezpieczeństwa informacji
* podział obowiązków
* odpowiedzialności kierownictwa
* kontakt z organami władzy
* kontakt z grupami szczególnego interesu
* analiza zagrożeń
* bezpieczeństwo informacji w zarządzaniu projektami
* rejestr informacji i innych powiązanych zasobów
* dopuszczalne wykorzystanie informacji i innych powiązanych zasobów
* zwrot zasobów
* klasyfikacja informacji
* oznakowanie informacji
* transfer informacji
* kontrola dostępu
* zarządzanie tożsamością
* informacje uwierzytelniające
* prawa dostępu
* bezpieczeństwo informacji w relacjach z dostawcami
* uwzględnianie bezpieczeństwa informacji w umowach z dostawcami
* zarządzanie bezpieczeństwem informacji w łańcuchu dostaw technologii informacyjnych i komunikacyjnych (ICT)
* monitorowanie, przegląd i zarządzanie zmianami w usługach dostawców
* bezpieczeństwo informacji przy korzystaniu z usług w chmurze
* planowanie i przygotowanie zarządzania incydentami bezpieczeństwa informacji
* ocena i decyzje dotyczące zdarzeń związanych z bezpieczeństwem informacji
* reagowanie na incydenty związane z bezpieczeństwem informacji
* wyciąganie wniosków z incydentów bezpieczeństwa informacji
* gromadzenie dowodów z naruszeń/incydentów związanych z bezpieczeństwem informacji
* bezpieczeństwo informacji w czasie zakłóceń związanych z bezpieczeństwem informacji
* gotowość technologii informacyjno- komunikacyjnych do zapewnienia ciągłości działania
* wymagania prawne, ustawowe, regulacyjne i umowne związanych z bezpieczeństwem informacji
* prawa własności intelektualnej
* ochrona zapisów
* prywatność i ochrona danych osobowych (PII)
* niezależny przegląd bezpieczeństwa informacji
* zgodność z polityką, zasadami i normami dotyczącymi bezpieczeństwa informacji
* udokumentowane procedury operacyjne

1. Obszaru 2: Zabezpieczenia zasobów ludzkich

* screening
* zasady i warunki zatrudnienia
* świadomość, edukacja i szkolenie w zakresie bezpieczeństwa
* postępowanie dyscyplinarne w konsekwencji naruszeń / incydentów związanych z bezpieczeństwem informacji
* obowiązki po rozwiązaniu lub zmianie zatrudnienia
* umowy o poufności lub nieujawnianiu informacji
* praca zdalna
* raportowanie zdarzeń dotyczących bezpieczeństwa informacji

1. Obszaru 3: Zabezpieczenia fizyczne

* strefy bezpieczeństwa fizycznego
* dostęp fizyczny
* zabezpieczanie biur, pomieszczeń i obiektów
* monitorowanie bezpieczeństwa fizycznego
* ochrona przed zagrożeniami fizycznymi i środowiskowymi
* praca w obszarach chronionych
* czyste biurko i czysty ekran
* rozmieszczenie i ochrona urządzeń
* bezpieczeństwo zasobów poza siedzibą firmy / organizacji
* nośniki danych
* urządzenia wspomagające
* bezpieczeństwo okablowania
* konserwacja sprzętu
* bezpieczna utylizacja lub ponowne wykorzystanie sprzętu

1. Obszaru 4: Zabezpieczenia technologiczne

* urządzenia końcowe użytkownika
* prawa uprzywilejowanego dostępu
* ograniczenie dostępu do informacji
* dostęp do kodu źródłowego
* bezpieczne uwierzytelnianie
* zarządzanie wydajnością
* ochrona przed złośliwym oprogramowaniem
* zarządzanie lukami technicznymi
* zarządzanie konfiguracją
* usuwanie informacji
* maskowanie danych
* zapobieganie wyciekom danych
* kopia zapasowa informacji
* nadmiarowość urządzeń do przetwarzania informacji
* rejestrowanie zdarzeń
* monitorowanie działań
* synchronizacja zegarów
* użycie uprzywilejowanych programów narzędziowych
* instalacja oprogramowania na systemach operacyjnych
* bezpieczeństwo sieci
* bezpieczeństwo usług sieciowych
* rozdzielenie sieci
* filtrowanie stron internetowych
* zastosowanie kryptografii
* cykl życia oprogramowania (SDLC)
* wymagania dotyczące bezpieczeństwa aplikacji
* architektura i zasady inżynierii bezpiecznych systemów
* bezpieczne kodowanie
* testy bezpieczeństwa w fazie rozwoju i akceptacji
* zlecone prace rozwojowe
* oddzielenie środowisk rozwojowych, testowych i produkcyjnych
* zarządzanie zmianą
* dane testowe
* ochrona systemów informatycznych podczas audytu

1. W przypadku stwierdzenia w trakcie opracowania wymaganych dokumentów jako zasady/zapisy/wymagania dane zabezpieczenie z w/w listy nie jest stosowane w organizacji Wykonawca przedstawia dodatkowy dokument w postaci raportu wykluczeń zabezpieczeń z dokładnym i precyzyjnym uzasadnieniem odstąpienia z opracowania wymagań dla takiego zabezpieczenia opisującym źródło takiej decyzji.
2. Dokumentacja SZBI musi obejmować swoim zakresem zagadnienia z obszarów System Zarządzania Bezpieczeństwem Informacji (SZBI), Ochrona (OCH), Zdarzenia i Monitoring (CM), Reagowanie (RE), Odtwarzanie (OD) załącznika nr 6\_Ankieta Dojrzałości Cyberbezpieczeństwa w JST do regulaminu konkursu grantowego Cyberbezpieczny Samorząd, stanowiący załącznik nr 1a do Zapytania Ofertowego.
3. Zamawiający nie dopuszcza kopiowania treści ogólnodostępnych w formie nieprzetworzonej (dostępnych w Internecie). Dokumenty będą zawierać przywołania zamiast cytowania tekstów analizowanych i powszechnie dostępnych. Dokumentacja ma zawierać wyłącznie autorskie treści, powstałe w wyniku realizacji zamówienia oraz inne autorskie treści wykonawcy, które nie są publicznie dostępne. Będą opracowaniem kompletnym, wyczerpującym i dostosowanym do potrzeb organizacji, z punktu widzenia celu, któremu mają służyć.
4. Zamawiający wymaga wdrożenia dokumentów do stosowania, a w szczególności:
5. Przygotowanie i przekazanie wytycznych odnośnie do elektronicznego nadzorowania dokumentów i zapisów, jeżeli potrzebne, konfiguracja ustawień
6. Uzupełnienia zapisów wymaganych normą razem z Zamawiającym
7. Konsultacje indywidualne z zakresu stosowania opracowanej dokumentacji
8. Udzielenie wszelkiego wsparcia w celu uzyskania biegłego posługiwania się przez Zamawiającego systemem (nie miej niż 20 godzin)

**Zakres audytu końcowego**

1. Audyt końcowy dotyczy Urzędu Miejskiego w Rabce Zdrój oraz 14 Jednostek Organizacyjnych.
2. Audyt ma na celu weryfikację poziomu spełnienia wymagań normy PN-ISO/IEC 27001:2023 przez Zamawiającego, w tym ocenę skuteczności zabezpieczeń technicznych, organizacyjnych i prawnych stosowanych u Zamawiającego, w wszystkich obszarach określonych załącznikiem A do ww. normy.
3. Przeprowadzenie audytu bezpieczeństwa w oparciu o wymagania załącznika A do normy ISO27001 oraz wytycznych normy ISO27002 w zakresie bezpieczeństwa systemów informatycznych wykorzystywanych do świadczenia usług dla klientów jednostek.
4. Audyt powinien zawierać także wskazania podatności systemów informatycznych: wskazanie podatności, wagi podatności, opis podatności, informacje dotyczące podatności w tym źródła zewnętrzne, rekomendacje co do sposobu postępowania.
5. Po zakończeniu audytu Wykonawca przygotuje i przekaże w raport z przeprowadzonego audytu oraz wypełnioną „Ankietę Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego", o których mowa w Regulaminie Konkursu Grantowego pn. „Cyberbezpieczny Samorząd” opublikowanym na stronie Centrum Projektów Polska Cyfrowa pod adresem <http://www.gov.pl/cppc/cyberbezpieczny-samorzad>.