

**Załącznik nr 1 do zapytania ofertowego****Opracowanie oraz wdrożenie dokumentacji SZBI dla Urzędu  
i jednostek organizacyjnych Gminy, usługi doradcze  
oraz szkolenia**

**Opis przedmiotu zamówienia na opracowanie wraz z wdrożeniem dokumentacji SZBI w Urzędzie Gminy Lubiszyn, realizowanie działań wspomagających realizację projektu – usługi doradcze, opracowanie wraz z wdrożeniem dokumentacji SZBI dla Szkoły Podstawowej im. Polskich Olimpijczyków w Baczynie, opracowanie wraz z wdrożeniem dokumentacji SZBI dla Szkoły Podstawowej im. Jana Pawła II w Lubiszynie, opracowanie wraz z wdrożeniem dokumentacji SZBI dla Szkoły Podstawowej w Stawie, opracowanie wraz z wdrożeniem dokumentacji SZBI dla Szkoły Podstawowej im. Tadeusza Kościuszki w Ściechowie, Opracowanie wraz z wdrożeniem dokumentacji SZBI dla Przedszkola w Buczynie i Przedszkola Gminnego w Lubiszynie, opracowanie wraz z wdrożeniem dokumentacji SZBI dla Zakładu Usług Komunalnych w Lubiszynie, szkolenie z zakresu cyberbezpieczeństwa dla pracowników oświaty**

**1. Opracowanie wraz z wdrożeniem dokumentacji SZBI w Urzędzie Gminy w Lubiszynie.**

W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do aktualizacji dokumentacji z zakresu bezpieczeństwa informacji posiadanej przez Zamawiającego oraz opracowania i wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Szczegółowy opis realizowanych w ramach zamówienia czynności związanych z wdrożeniem dokumentacji systemu zarządzania bezpieczeństwem informacji:

1. W ramach wykonywanych prac Wykonawca zapewni zgodność dokumentacji z poniższymi wymaganiami:
  - a. 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;
  - b. ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa wraz z nowelizacjami ustawy, które zostaną dokonane w czasie realizacji zamówienia;
  - c. 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);

- d. wymagania norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005 i w oparciu o główne założenia norm ISO 31000 w zakresie zarządzania ryzykiem oraz PN-EN ISO 22301 w zakresie ciągłości działania;
  - e. wymagania regulaminu konkursu grantowego oraz umowy o powierzenie grantu zawartej w ramach projektu „Cyberbezpieczny Samorząd”.
2. Wdrażany System Zarządzania Bezpieczeństwem Informacji powinien składać się z obszarów regulujących następujące obszary:
- a. zarządzanie aktywami,
  - b. zarządzanie ryzykiem,
  - c. zapewnienie bezpieczeństwa systemów informatycznych oraz ich rozwoju,
  - d. zapewnienie bezpieczeństwa fizycznego,
  - e. kontrola dostępu do oprogramowania i infrastruktury sieciowej,
  - f. klasyfikacja informacji oraz nadzoru nad dokumentacją,
  - g. zapewnienie bezpieczeństwa zasobów ludzkich,
  - h. wykonywanie kopii zapasowych,
  - i. stosowanie kryptografii,
  - j. obsługa incydentów i realizacja działań korygujących,
  - k. prowadzenie wewnętrznych audytów bezpieczeństwa,
  - l. prowadzenie przeglądów zarządzania,
  - m. zapewnienie ciągłości działania i przywracania normalnej działalności po wystąpieniu zakłóceń,
  - n. zapewnienie bezpieczeństwa łańcucha dostaw,
  - o. postępowanie z podatnościami systemów i sieci,
  - p. Deklaracja stosowania (w oparciu o załącznik A do normy ISO/IEC 27001:2022).
3. W ramach wdrażania Systemu Zarządzania Bezpieczeństwem Informacji powinny zostać uregulowane zabezpieczenia określone w załączniku A do normy ISO/IEC 27001:2022:
- a. Zabezpieczenia organizacyjne
    - i. Polityki bezpieczeństwa informacji
    - ii. Role i obowiązki w zakresie bezpieczeństwa informacji
    - iii. Rozdzielenie obowiązków
    - iv. Odpowiedzialność kierownictwa
    - v. Kontakty z organami władzy
    - vi. Kontakty z grupami zainteresowanych specjalistów
    - vii. Informacja o zagrożeniach
    - viii. Bezpieczeństwo informacji w zarządzaniu projektami
    - ix. Inwentaryzacja informacji i innych powiązanych aktywów
    - x. Akceptowalne użycie informacji i innych powiązanych aktywów
    - xi. Zwrot aktywów
    - xii. Klasyfikacja informacji
    - xiii. Oznaczanie informacji
    - xiv. Przesyłanie informacji
    - xv. Kontrola dostępu

- xvi. Zarządzanie tożsamością (prawami dostępu)
- xvii. Informacje uwierzytelniające
- xviii. Prawa dostępu
- xix. Bezpieczeństwo informacji w relacjach z dostawcami
- xx. Uwzględnienie bezpieczeństwa informacji w umowach z dostawcami
- xxi. Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw technologii informacyjno-komunikacyjnych (ICT)
- xxii. Monitorowanie, przegląd i zarządzanie zmianą usług świadczonych przez dostawców
- xxiii. Bezpieczeństwo informacji w usłudze chmury
- xxiv. Planowanie i przygotowywanie się do zarządzania incydentami bezpieczeństwa informacji
- xxv. Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji
- xxvi. Reagowanie na incydenty bezpieczeństwa informacji
- xxvii. Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji
- xxviii. Gromadzenie materiałów dowodowych
- xxix. Bezpieczeństwo informacji podczas zakłóceń
- xxx. Gotowość teleinformatyczna do zapewnienia ciągłości działania
- xxxi. Wymogi prawne, ustawowe, regulacyjne i umowne
- xxxii. Prawa własności intelektualnej
- xxxiii. Ochrona zapisów
- xxxiv. Prywatność i ochrona danych osobowych (PII)
- xxxv. Niezależny przegląd bezpieczeństwa informacji
- xxxvi. Zgodność z politykami, zasadami i standardami bezpieczeństwa informacji
- xxxvii. Dokumentowanie procedur operacyjnych

b. Zabezpieczenia związane z ludźmi

- i. Postępowanie sprawdzające
- ii. Warunki zatrudnienia
- iii. Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
- iv. Postępowania dyscyplinarne
- v. Zakończenie zatrudnienia lub zmiana zakresu obowiązków
- vi. Umowy o zachowaniu poufności
- vii. Praca zdalna
- viii. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji

c. Zabezpieczenia fizyczne

- i. Fizyczna granica obszaru bezpiecznego
- ii. Zabezpieczenie fizycznych wejść
- iii. Zabezpieczenie biur, pomieszczeń i obiektów
- iv. Monitorowanie bezpieczeństwa fizycznego
- v. Ochrona przed zagrożeniami fizycznymi i środowiskowymi

- vi. Praca w obszarach bezpiecznych
- vii. Polityka czystego biurka i czystego ekranu
- viii. Lokalizacja i ochrona sprzętu
- ix. Bezpieczeństwo sprzętu i aktywów poza siedzibą
- x. Zarządzanie nośnikami danych
- xi. Systemy wspomagające
- xii. Bezpieczeństwo okablowania
- xiii. Konserwacja sprzętu
- xiv. Bezpieczne zbywanie lub przekazywanie do ponownego użycia

d. Zabezpieczenia technologiczne

- i. Urządzenia końcowe użytkowników
- ii. Uprzywilejowane prawa dostępu
- iii. Ograniczenie dostępu do informacji
- iv. Dostęp do kodów źródłowych
- v. Bezpieczne uwierzytelnienie
- vi. Zarządzanie pojemnością
- vii. Zabezpieczenie przed szkodliwym oprogramowaniem
- viii. Zarządzanie podatnościami technicznymi
- ix. Zarządzanie konfiguracją
- x. Usuwanie informacji
- xi. Maskowanie danych
- xii. Zapobieganie wyciekom danych
- xiii. Zapasowe kopie bezpieczeństwa
- xiv. Redundancja środków przetwarzania informacji
- xv. Rejestrowanie działań
- xvi. Działania monitorujące
- xvii. Synchronizacja zegarów
- xviii. Użycie uprzywilejowanych programów narzędziowych
- xix. Instalacja oprogramowania w systemach operacyjnych
- xx. Zabezpieczenia sieci
- xxi. Bezpieczeństwo usług sieciowych
- xxii. Rozdzielenie sieci
- xxiii. Filtrowanie stron internetowych
- xxiv. Użycie kryptografii
- xxv. Bezpieczeństwo prac rozwojowych
- xxvi. Wymagania bezpieczeństwa aplikacji
- xxvii. Zasady projektowania bezpiecznych systemów
- xxviii. Bezpieczne programowanie
- xxix. Testowanie bezpieczeństwa w fazie rozwoju i akceptacja
- xxx. Outsourcing prac rozwojowych

- xxxi. Rozdzielenie środowisk deweloperskich, testowych i produkcyjnych
  - xxxii. Zarządzanie zmianami
  - xxxiii. Ochrona danych testowych
  - xxxiv. Ochrona systemów informatycznych podczas testów audytowych
4. W toku wdrażania dokumentacji nie mogą zostać przekazane Zamawiającemu puste druki (wzorce) dokumentów, jednakże ich wdrożenie powinno opierać się na wypełnieniu wdrażanej dokumentacji zgodnie ze stanem przypadającym na okres wdrożenia. Zamawiający deklaruje przekazywanie niezbędnych danych Wykonawcy, jednakże Wykonawca powinien odpowiednio wdrożyć zapisy do dokumentów przekazywanych Zamawiającemu.
  5. W toku wdrażania dokumentacji u Zamawiającego Wykonawca zobowiązany jest do zapewnienia dostępności osób wskazanych w wykazie osób, w ramach prowadzonego postępowania, w siedzibie Zamawiającego przez okres minimum 5 godzin.
  6. Zamawiający wymaga, żeby zapisy dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji odnosiły się do wymagań norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005. Dokumentacja powinna być przygotowana w oparciu o wytyczne wynikające z norm ISO 31000 w zakresie zarządzania ryzykiem oraz zarządzania ciągłością działania PN-EN ISO 22301. Zamawiający dokona weryfikacji zgodności na etapie odbioru dokumentacji. W przypadku wykrycia niezgodności Wykonawca będzie zobowiązany do wprowadzenia poprawek zgodnych z wolą Zamawiającego, przy czym wprowadzane poprawki będą realizowane w ramach zawartej umowy, bez dodatkowego wynagrodzenia.
  7. Wykonawca w ramach realizacji umowy zapewni przez cały okres realizacji umowy wsparcie Pełnomocnika ds. SZBI, który będzie dostępny zdalnie na żądanie pracowników Zamawiającego w zakresie prawidłowego wykorzystywania dokumentacji systemu zarządzania bezpieczeństwem informacji. Możliwość wsparcia Pełnomocnika ds. SZBI powinna zostać zapewniona w ciągu 5 dni roboczych od zgłoszenia potrzeby pracowników Zamawiającego.

## **2. Realizowanie działań wspomagających realizację projektu – usługi doradcze.**

W ramach realizowanego przedmiotu zamówienia polegającego na wsparciu doradczym w zakresie merytorycznego wsparcia realizacji projektu, Wykonawca jest zobowiązany do zapewnienia wsparcia Zamawiającego w zakresie zapewnienia wzrostu poziomu cyberbezpieczeństwa w związku z realizacją projektu.

Do obowiązków Wykonawcy podczas realizacji wsparcia doradczego w zakresie cyberbezpieczeństwa będzie należało:

- a) przeprowadzanie konsultacji z Zamawiającym na każdym etapie prac, dotyczące istotnych elementów mających wpływ na zwiększenie cyberbezpieczeństwa, poprzez przetestowanie podatności w ramach infrastruktury sieciowej urzędu oraz wybranych przez Zamawiającego jednostek organizacyjnych (minimum dwie jednostki) – testowanie podatności musi zostać zrealizowane fizycznie w siedzibie urzędu oraz jednostek organizacyjnych;
- b) doradztwo merytoryczne w trakcie wypełniania przez Zamawiającego ankiety potwierdzającej osiągnięcie celów bezpieczeństwa określonych w projekcie.

Wsparcie doradcze będzie realizowane przez Wykonawcę w formie zdalnej oraz stacjonarnej, przy czym przyjmuje się, iż przez cały okres realizacji umowy Wykonawca pojawi się fizycznie minimum 2 razy w siedzibie Zamawiającego, a łączna liczba godzin zrealizowanych w ramach doradztwa wyniesienie 20 godzin (zarówno zdalnych jak i realizowanych w siedzibie Zamawiającego). Dodatkowo Wykonawca będzie zobowiązany do pojawienia się w siedzibie Zamawiającego na wezwanie w terminie 2 dni.

Wykonawca zrealizuje również weryfikację osiągnięcia celów projektu poprzez przetestowanie podatności infrastruktury sieciowej urzędu, czyli weryfikację fizyczną wdrożonych rozwiązań i ich funkcjonowania w urzędzie oraz w jednostkach organizacyjnych (minimum dwóch), a także przekaze Zamawiającemu raport z wykonanej weryfikacji.

### **3. Opracowanie wraz z wdrożeniem dokumentacji SZBI dla Szkoły Podstawowej im. Polskich Olimpijczyków w Baczynie.**

W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do aktualizacji dokumentacji z zakresu bezpieczeństwa informacji posiadanej przez Zamawiającego oraz opracowania i wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Szczegółowy opis realizowanych w ramach zamówienia czynności związanych z wdrożeniem dokumentacji systemu zarządzania bezpieczeństwem informacji:

1. W ramach wykonywanych prac Wykonawca zapewni zgodność dokumentacji z poniższymi wymaganiami:
  - a. 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;
  - b. ustawa z dnia z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa wraz z nowelizacjami ustawy, które zostaną dokonane w czasie realizacji zamówienia;
  - c. 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);
  - d. wymagania norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005 i w oparciu o główne założenia norm ISO 31000 w zakresie zarządzania ryzykiem oraz PN-EN ISO 22301 w zakresie ciągłości działania;
  - e. wymagania regulaminu konkursu grantowego oraz umowy o powierzenie grantu zawartej w ramach projektu „Cyberbezpieczny Samorząd”.
2. Wdrażany System Zarządzania Bezpieczeństwem Informacji powinien składać się z obszarów regulujących następujące obszary:
  - a. zarządzanie aktywami,
  - b. zarządzanie ryzykiem,
  - c. zapewnienie bezpieczeństwa systemów informatycznych oraz ich rozwoju,
  - d. zapewnienie bezpieczeństwa fizycznego,
  - e. kontrola dostępu do oprogramowania i infrastruktury sieciowej,

- f. klasyfikacja informacji oraz nadzoru nad dokumentacją,
  - g. zapewnienie bezpieczeństwa zasobów ludzkich,
  - h. wykonywanie kopii zapasowych,
  - i. stosowanie kryptografii,
  - j. obsługa incydentów i realizacja działań korygujących,
  - k. prowadzenie wewnętrznych audytów bezpieczeństwa,
  - l. prowadzenie przeglądów zarządzania,
  - m. zapewnienie ciągłości działania i przywracania normalnej działalności po wystąpieniu zakłóceń,
  - n. zapewnienie bezpieczeństwa łańcucha dostaw,
  - o. postępowanie z podatnościami systemów i sieci,
  - p. Deklaracja stosowania (w oparciu o załącznik A do normy ISO/IEC 27001:2022).
3. W ramach wdrażania Systemu Zarządzania Bezpieczeństwem Informacji powinny zostać uregulowane zabezpieczenia określone w załączniku A do normy ISO/IEC 27001:2022:
- a. Zabezpieczenia organizacyjne
    - i. Polityki bezpieczeństwa informacji
    - ii. Role i obowiązki w zakresie bezpieczeństwa informacji
    - iii. Rozdzielenie obowiązków
    - iv. Odpowiedzialność kierownictwa
    - v. Kontakty z organami władzy
    - vi. Kontakty z grupami zainteresowanych specjalistów
    - vii. Informacja o zagrożeniach
    - viii. Bezpieczeństwo informacji w zarządzaniu projektami
    - ix. Inwentaryzacja informacji i innych powiązanych aktywów
    - x. Akceptowalne użycie informacji i innych powiązanych aktywów
    - xi. Zwrot aktywów
    - xii. Klasyfikacja informacji
    - xiii. Oznaczanie informacji
    - xiv. Przesyłanie informacji
    - xv. Kontrola dostępu
    - xvi. Zarządzanie tożsamością (prawami dostępu)
    - xvii. Informacje uwierzytelniające
    - xviii. Prawa dostępu
    - xix. Bezpieczeństwo informacji w relacjach z dostawcami
    - xx. Uwzględnienie bezpieczeństwa informacji w umowach z dostawcami
    - xxi. Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw technologii informacyjno-komunikacyjnych (ICT)
    - xxii. Monitorowanie, przegląd i zarządzanie zmianą usług świadczonych przez dostawców
    - xxiii. Bezpieczeństwo informacji w usłudze chmury
    - xxiv. Planowanie i przygotowywanie się do zarządzania incydentami bezpieczeństwa informacji
    - xxv. Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji

- xxvi. Reagowanie na incydenty bezpieczeństwa informacji
- xxvii. Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji
- xxviii. Gromadzenie materiałów dowodowych
- xxix. Bezpieczeństwo informacji podczas zakłóceń
- xxx. Gotowość teleinformatyczna do zapewnienia ciągłości działania
- xxxi. Wymogi prawne, ustawowe, regulacyjne i umowne
- xxxii. Prawa własności intelektualnej
- xxxiii. Ochrona zapisów
- xxxiv. Prywatność i ochrona danych osobowych (PII)
- xxxv. Niezależny przegląd bezpieczeństwa informacji
- xxxvi. Zgodność z politykami, zasadami i standardami bezpieczeństwa informacji
- xxxvii. Dokumentowanie procedur operacyjnych

b. Zabezpieczenia związane z ludźmi

- i. Postępowanie sprawdzające
- ii. Warunki zatrudnienia
- iii. Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
- iv. Postępowania dyscyplinarne
- v. Zakończenie zatrudnienia lub zmiana zakresu obowiązków
- vi. Umowy o zachowaniu poufności
- vii. Praca zdalna
- viii. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji

c. Zabezpieczenia fizyczne

- i. Fizyczna granica obszaru bezpiecznego
- ii. Zabezpieczenie fizycznych wejść
- iii. Zabezpieczenie biur, pomieszczeń i obiektów
- iv. Monitorowanie bezpieczeństwa fizycznego
- v. Ochrona przed zagrożeniami fizycznymi i środowiskowymi
- vi. Praca w obszarach bezpiecznych
- vii. Polityka czystego biurka i czystego ekranu
- viii. Lokalizacja i ochrona sprzętu
- ix. Bezpieczeństwo sprzętu i aktywów poza siedzibą
- x. Zarządzanie nośnikami danych
- xi. Systemy wspomagające
- xii. Bezpieczeństwo okablowania
- xiii. Konserwacja sprzętu
- xiv. Bezpieczne zbywanie lub przekazywanie do ponownego użycia

d. Zabezpieczenia technologiczne

- i. Urządzenia końcowe użytkowników



- ii. Uprzywilejowane prawa dostępu
  - iii. Ograniczenie dostępu do informacji
  - iv. Dostęp do kodów źródłowych
  - v. Bezpieczne uwierzytelnienie
  - vi. Zarządzanie pojemnością
  - vii. Zabezpieczenie przed szkodliwym oprogramowaniem
  - viii. Zarządzanie podatnościami technicznymi
  - ix. Zarządzanie konfiguracją
  - x. Usuwanie informacji
  - xi. Maskowanie danych
  - xii. Zapobieganie wyciekom danych
  - xiii. Zapasowe kopie bezpieczeństwa
  - xiv. Redundancja środków przetwarzania informacji
  - xv. Rejestrowanie działań
  - xvi. Działania monitorujące
  - xvii. Synchronizacja zegarów
  - xviii. Użycie uprzywilejowanych programów narzędziowych
  - xix. Instalacja oprogramowania w systemach operacyjnych
  - xx. Zabezpieczenia sieci
  - xxi. Bezpieczeństwo usług sieciowych
  - xxii. Rozdzielenie sieci
  - xxiii. Filtrowanie stron internetowych
  - xxiv. Użycie kryptografii
  - xxv. Bezpieczeństwo prac rozwojowych
  - xxvi. Wymagania bezpieczeństwa aplikacji
  - xxvii. Zasady projektowania bezpiecznych systemów
  - xxviii. Bezpieczne programowanie
  - xxix. Testowanie bezpieczeństwa w fazie rozwoju i akceptacja
  - xxx. Outsourcing prac rozwojowych
  - xxxi. Rozdzielenie środowisk deweloperskich, testowych i produkcyjnych
  - xxxii. Zarządzanie zmianami
  - xxxiii. Ochrona danych testowych
  - xxxiv. Ochrona systemów informatycznych podczas testów audytowych
4. W toku wdrażania dokumentacji nie mogą zostać przekazane Zamawiającemu puste druki (wzorce) dokumentów, jednakże ich wdrożenie powinno opierać się na wypełnieniu wdrażanej dokumentacji zgodnie ze stanem przypadającym na okres wdrożenia. Zamawiający deklaruje przekazywanie niezbędnych danych Wykonawcy, jednakże Wykonawca powinien odpowiednio wdrożyć zapisy do dokumentów przekazywanych Zamawiającemu.
5. W toku wdrażania dokumentacji u Zamawiającego Wykonawca zobowiązany jest do zapewnienia dostępności osób wskazanych w wykazie osób, w ramach prowadzonego postępowania, w siedzibie Zamawiającego przez okres minimum 5 godzin.

6. Zamawiający wymaga, żeby zapisy dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji odnosiły się do wymagań norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005. Dokumentacja powinna być przygotowana w oparciu o wytyczne wynikające z norm ISO 31000 w zakresie zarządzania ryzykiem oraz zarządzania ciągłością działania PN-EN ISO 22301. Zamawiający dokona weryfikacji zgodności na etapie odbioru dokumentacji. W przypadku wykrycia niezgodności Wykonawca będzie zobowiązany do wprowadzenia poprawek zgodnych z wolą Zamawiającego, przy czym wprowadzane poprawki będą realizowane w ramach zawartej umowy, bez dodatkowego wynagrodzenia.
7. Wykonawca w ramach realizacji umowy zapewni przez cały okres realizacji umowy wsparcie Pełnomocnika ds. SZBI, który będzie dostępny zdalnie na żądanie pracowników Zamawiającego w zakresie prawidłowego wykorzystywania dokumentacji systemu zarządzania bezpieczeństwem informacji. Możliwość wsparcia Pełnomocnika ds. SZBI powinna zostać zapewniona w ciągu 5 dni roboczych od zgłoszenia potrzeby pracowników Zamawiającego.

#### **4. Opracowanie wraz z wdrożeniem dokumentacji SZBI dla Szkoły Podstawowej im. Jana Pawła II w Lubiszynie.**

W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do aktualizacji dokumentacji z zakresu bezpieczeństwa informacji posiadanej przez Zamawiającego oraz opracowania i wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Szczegółowy opis realizowanych w ramach zamówienia czynności związanych z wdrożeniem dokumentacji systemu zarządzania bezpieczeństwem informacji:

1. W ramach wykonywanych prac Wykonawca zapewni zgodność dokumentacji z poniższymi wymaganiami:
  - a. 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;
  - b. ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa wraz z nowelizacjami ustawy, które zostaną dokonane w czasie realizacji zamówienia;
  - c. 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);
  - d. wymagania norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005 i w oparciu o główne założenia norm ISO 31000 w zakresie zarządzania ryzykiem oraz PN-EN ISO 22301 w zakresie ciągłości działania;
  - e. wymagania regulaminu konkursu grantowego oraz umowy o powierzenie grantu zawartej w ramach projektu „Cyberbezpieczny Samorząd”.
2. Wdrażany System Zarządzania Bezpieczeństwem Informacji powinien składać się z obszarów regulujących następujące obszary:
  - a. zarządzanie aktywami,
  - b. zarządzanie ryzykiem,

- c. zapewnienie bezpieczeństwa systemów informatycznych oraz ich rozwoju,
  - d. zapewnienie bezpieczeństwa fizycznego,
  - e. kontrola dostępu do oprogramowania i infrastruktury sieciowej,
  - f. klasyfikacja informacji oraz nadzoru nad dokumentacją,
  - g. zapewnienie bezpieczeństwa zasobów ludzkich,
  - h. wykonywanie kopii zapasowych,
  - i. stosowanie kryptografii,
  - j. obsługa incydentów i realizacja działań korygujących,
  - k. prowadzenie wewnętrznych audytów bezpieczeństwa,
  - l. prowadzenie przeglądów zarządzania,
  - m. zapewnienie ciągłości działania i przywracania normalnej działalności po wystąpieniu zakłóceń,
  - n. zapewnienie bezpieczeństwa łańcucha dostaw,
  - o. postępowanie z podatnościami systemów i sieci,
  - p. Deklaracja stosowania (w oparciu o załącznik A do normy ISO/IEC 27001:2022).
3. W ramach wdrażania Systemu Zarządzania Bezpieczeństwem Informacji powinny zostać uregulowane zabezpieczenia określone w załączniku A do normy ISO/IEC 27001:2022:
- a. Zabezpieczenia organizacyjne
    - i. Polityki bezpieczeństwa informacji
    - ii. Role i obowiązki w zakresie bezpieczeństwa informacji
    - iii. Rozdzielenie obowiązków
    - iv. Odpowiedzialność kierownictwa
    - v. Kontakty z organami władzy
    - vi. Kontakty z grupami zainteresowanych specjalistów
    - vii. Informacja o zagrożeniach
    - viii. Bezpieczeństwo informacji w zarządzaniu projektami
    - ix. Inwentaryzacja informacji i innych powiązanych aktywów
    - x. Akceptowalne użycie informacji i innych powiązanych aktywów
    - xi. Zwrot aktywów
    - xii. Klasyfikacja informacji
    - xiii. Oznaczanie informacji
    - xiv. Przesyłanie informacji
    - xv. Kontrola dostępu
    - xvi. Zarządzanie tożsamością (prawami dostępu)
    - xvii. Informacje uwierzytelniające
    - xviii. Prawa dostępu
    - xix. Bezpieczeństwo informacji w relacjach z dostawcami
    - xx. Uwzględnienie bezpieczeństwa informacji w umowach z dostawcami
    - xxi. Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw technologii informacyjno-komunikacyjnych (ICT)
    - xxii. Monitorowanie, przegląd i zarządzanie zmianą usług świadczonych przez dostawców
    - xxiii. Bezpieczeństwo informacji w usłudze chmury

- xxiv. Planowanie i przygotowywanie się do zarządzania incydentami bezpieczeństwa informacji
- xxv. Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji
- xxvi. Reagowanie na incydenty bezpieczeństwa informacji
- xxvii. Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji
- xxviii. Gromadzenie materiałów dowodowych
- xxix. Bezpieczeństwo informacji podczas zakłóceń
- xxx. Gotowość teleinformatyczna do zapewnienia ciągłości działania
- xxxi. Wymogi prawne, ustawowe, regulacyjne i umowne
- xxxii. Prawa własności intelektualnej
- xxxiii. Ochrona zapisów
- xxxiv. Prywatność i ochrona danych osobowych (PII)
- xxxv. Niezależny przegląd bezpieczeństwa informacji
- xxxvi. Zgodność z politykami, zasadami i standardami bezpieczeństwa informacji
- xxxvii. Dokumentowanie procedur operacyjnych

b. Zabezpieczenia związane z ludźmi

- i. Postępowanie sprawdzające
- ii. Warunki zatrudnienia
- iii. Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
- iv. Postępowania dyscyplinarne
- v. Zakończenie zatrudnienia lub zmiana zakresu obowiązków
- vi. Umowy o zachowaniu poufności
- vii. Praca zdalna
- viii. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji

c. Zabezpieczenia fizyczne

- i. Fizyczna granica obszaru bezpiecznego
- ii. Zabezpieczenie fizycznych wejść
- iii. Zabezpieczenie biur, pomieszczeń i obiektów
- iv. Monitorowanie bezpieczeństwa fizycznego
- v. Ochrona przed zagrożeniami fizycznymi i środowiskowymi
- vi. Praca w obszarach bezpiecznych
- vii. Polityka czystego biurka i czystego ekranu
- viii. Lokalizacja i ochrona sprzętu
- ix. Bezpieczeństwo sprzętu i aktywów poza siedzibą
- x. Zarządzanie nośnikami danych
- xi. Systemy wspomagające
- xii. Bezpieczeństwo okablowania
- xiii. Konserwacja sprzętu
- xiv. Bezpieczne zbywanie lub przekazywanie do ponownego użycia



- d. Zabezpieczenia technologiczne
  - i. Urządzenia końcowe użytkowników
  - ii. Uprzywilejowane prawa dostępu
  - iii. Ograniczenie dostępu do informacji
  - iv. Dostęp do kodów źródłowych
  - v. Bezpieczne uwierzytelnienie
  - vi. Zarządzanie pojemnością
  - vii. Zabezpieczenie przed szkodliwym oprogramowaniem
  - viii. Zarządzanie podatnościami technicznymi
  - ix. Zarządzanie konfiguracją
  - x. Usuwanie informacji
  - xi. Maskowanie danych
  - xii. Zapobieganie wyciekom danych
  - xiii. Zapasowe kopie bezpieczeństwa
  - xiv. Redundancja środków przetwarzania informacji
  - xv. Rejestrowanie działań
  - xvi. Działania monitorujące
  - xvii. Synchronizacja zegarów
  - xviii. Użycie uprzywilejowanych programów narzędziowych
  - xix. Instalacja oprogramowania w systemach operacyjnych
  - xx. Zabezpieczenia sieci
  - xxi. Bezpieczeństwo usług sieciowych
  - xxii. Rozdzielenie sieci
  - xxiii. Filtrowanie stron internetowych
  - xxiv. Użycie kryptografii
  - xxv. Bezpieczeństwo prac rozwojowych
  - xxvi. Wymagania bezpieczeństwa aplikacji
  - xxvii. Zasady projektowania bezpiecznych systemów
  - xxviii. Bezpieczne programowanie
  - xxix. Testowanie bezpieczeństwa w fazie rozwoju i akceptacja
  - xxx. Outsourcing prac rozwojowych
  - xxxi. Rozdzielenie środowisk deweloperskich, testowych i produkcyjnych
  - xxxii. Zarządzanie zmianami
  - xxxiii. Ochrona danych testowych
  - xxxiv. Ochrona systemów informatycznych podczas testów audytowych
- 4. W toku wdrażania dokumentacji nie mogą zostać przekazane Zamawiającemu puste druki (wzorce) dokumentów, jednakże ich wdrożenie powinno opierać się na wypełnieniu wdrażanej dokumentacji zgodnie ze stanem przypadającym na okres wdrożenia. Zamawiający deklaruje przekazywanie niezbędnych danych Wykonawcy, jednakże Wykonawca powinien odpowiednio wdrożyć zapisy do dokumentów przekazywanych Zamawiającemu.

5. W toku wdrażania dokumentacji u Zamawiającego Wykonawca zobowiązany jest do zapewnienia dostępności osób wskazanych w wykazie osób, w ramach prowadzonego postępowania, w siedzibie Zamawiającego przez okres minimum 5 godzin.
6. Zamawiający wymaga, żeby zapisy dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji odnosiły się do wymagań norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005. Dokumentacja powinna być przygotowana w oparciu o wytyczne wynikające z norm ISO 31000 w zakresie zarządzania ryzykiem oraz zarządzania ciągłością działania PN-EN ISO 22301. Zamawiający dokona weryfikacji zgodności na etapie odbioru dokumentacji. W przypadku wykrycia niezgodności Wykonawca będzie zobowiązany do wprowadzenia poprawek zgodnych z wolą Zamawiającego, przy czym wprowadzane poprawki będą realizowane w ramach zawartej umowy, bez dodatkowego wynagrodzenia.
7. Wykonawca w ramach realizacji umowy zapewni przez cały okres realizacji umowy wsparcie Pełnomocnika ds. SZBI, który będzie dostępny zdalnie na żądanie pracowników Zamawiającego w zakresie prawidłowego wykorzystywania dokumentacji systemu zarządzania bezpieczeństwem informacji. Możliwość wsparcia Pełnomocnika ds. SZBI powinna zostać zapewniona w ciągu 5 dni roboczych od zgłoszenia potrzeby pracowników Zamawiającego.

## **5. Opracowanie wraz z wdrożeniem dokumentacji SZBI dla Szkoły Podstawowej w Stawie.**

W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do aktualizacji dokumentacji z zakresu bezpieczeństwa informacji posiadanej przez Zamawiającego oraz opracowania i wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Szczegółowy opis realizowanych w ramach zamówienia czynności związanych z wdrożeniem dokumentacji systemu zarządzania bezpieczeństwem informacji:

1. W ramach wykonywanych prac Wykonawca zapewni zgodność dokumentacji z poniższymi wymaganiami:
  - a. 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;
  - b. ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa wraz z nowelizacjami ustawy, które zostaną dokonane w czasie realizacji zamówienia;
  - c. 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);
  - d. wymagania norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005 i w oparciu o główne założenia norm ISO 31000 w zakresie zarządzania ryzykiem oraz PN-EN ISO 22301 w zakresie ciągłości działania;
  - e. wymagania regulaminu konkursu grantowego oraz umowy o powierzenie grantu zawartej w ramach projektu „Cyberbezpieczny Samorząd”.

2. Wdrażany System Zarządzania Bezpieczeństwem Informacji powinien składać się z obszarów regulujących następujące obszary:
- zarządzanie aktywami,
  - zarządzanie ryzykiem,
  - zapewnienie bezpieczeństwa systemów informatycznych oraz ich rozwoju,
  - zapewnienie bezpieczeństwa fizycznego,
  - kontrola dostępu do oprogramowania i infrastruktury sieciowej,
  - klasyfikacja informacji oraz nadzoru nad dokumentacją,
  - zapewnienie bezpieczeństwa zasobów ludzkich,
  - wykonywanie kopii zapasowych,
  - stosowanie kryptografii,
  - obsługa incydentów i realizacja działań korygujących,
  - przewodzenie wewnętrznych audytów bezpieczeństwa,
  - przewodzenie przeglądów zarządzania,
  - zapewnienie ciągłości działania i przywracania normalnej działalności po wystąpieniu zakłóceń,
  - zapewnienie bezpieczeństwa łańcucha dostaw,
  - postępowanie z podatnościami systemów i sieci,
  - Deklaracja stosowania (w oparciu o załącznik A do normy ISO/IEC 27001:2022).
3. W ramach wdrażania Systemu Zarządzania Bezpieczeństwem Informacji powinny zostać uregulowane zabezpieczenia określone w załączniku A do normy ISO/IEC 27001:2022:
- Zabezpieczenia organizacyjne
    - Polityki bezpieczeństwa informacji
    - Role i obowiązki w zakresie bezpieczeństwa informacji
    - Rozdzielenie obowiązków
    - Odpowiedzialność kierownictwa
    - Kontakty z organami władzy
    - Kontakty z grupami zainteresowanych specjalistów
    - Informacja o zagrożeniach
    - Bezpieczeństwo informacji w zarządzaniu projektami
    - Inwentaryzacja informacji i innych powiązanych aktywów
    - Akceptowalne użycie informacji i innych powiązanych aktywów
    - Zwrot aktywów
    - Klasyfikacja informacji
    - Oznaczanie informacji
    - Przesyłanie informacji
    - Kontrola dostępu
    - Zarządzanie tożsamością (prawami dostępu)
    - Informacje uwierzytelniające
    - Prawa dostępu
    - Bezpieczeństwo informacji w relacjach z dostawcami
    - Uwzględnienie bezpieczeństwa informacji w umowach z dostawcami

- xxi. Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw technologii informacyjno-komunikacyjnych (ICT)
  - xxii. Monitorowanie, przegląd i zarządzanie zmianą usług świadczonych przez dostawców
  - xxiii. Bezpieczeństwo informacji w usłudze chmury
  - xxiv. Planowanie i przygotowywanie się do zarządzania incydentami bezpieczeństwa informacji
  - xxv. Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji
  - xxvi. Reagowanie na incydenty bezpieczeństwa informacji
  - xxvii. Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji
  - xxviii. Gromadzenie materiałów dowodowych
  - xxix. Bezpieczeństwo informacji podczas zakłóceń
  - xxx. Gotowość teleinformatyczna do zapewnienia ciągłości działania
  - xxxi. Wymogi prawne, ustawowe, regulacyjne i umowne
  - xxxii. Prawa własności intelektualnej
  - xxxiii. Ochrona zapisów
  - xxxiv. Prywatność i ochrona danych osobowych (PII)
  - xxxv. Niezależny przegląd bezpieczeństwa informacji
  - xxxvi. Zgodność z politykami, zasadami i standardami bezpieczeństwa informacji
  - xxxvii. Dokumentowanie procedur operacyjnych
- b. Zabezpieczenia związane z ludźmi
- i. Postępowanie sprawdzające
  - ii. Warunki zatrudnienia
  - iii. Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
  - iv. Postępowania dyscyplinarne
  - v. Zakończenie zatrudnienia lub zmiana zakresu obowiązków
  - vi. Umowy o zachowaniu poufności
  - vii. Praca zdalna
  - viii. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji
- c. Zabezpieczenia fizyczne
- i. Fizyczna granica obszaru bezpiecznego
  - ii. Zabezpieczenie fizycznych wejść
  - iii. Zabezpieczenie biur, pomieszczeń i obiektów
  - iv. Monitorowanie bezpieczeństwa fizycznego
  - v. Ochrona przed zagrożeniami fizycznymi i środowiskowymi
  - vi. Praca w obszarach bezpiecznych
  - vii. Polityka czystego biurka i czystego ekranu
  - viii. Lokalizacja i ochrona sprzętu
  - ix. Bezpieczeństwo sprzętu i aktywów poza siedzibą
  - x. Zarządzanie nośnikami danych



- xi. Systemy wspomagające
- xii. Bezpieczeństwo okablowania
- xiii. Konserwacja sprzętu
- xiv. Bezpieczne zbywanie lub przekazywanie do ponownego użycia

d. Zabezpieczenia technologiczne

- i. Urządzenia końcowe użytkowników
- ii. Uprzywilejowane prawa dostępu
- iii. Ograniczenie dostępu do informacji
- iv. Dostęp do kodów źródłowych
- v. Bezpieczne uwierzytelnienie
- vi. Zarządzanie pojemnością
- vii. Zabezpieczenie przed szkodliwym oprogramowaniem
- viii. Zarządzanie podatnościami technicznymi
- ix. Zarządzanie konfiguracją
- x. Usuwanie informacji
- xi. Maskowanie danych
- xii. Zapobieganie wyciekom danych
- xiii. Zapasowe kopie bezpieczeństwa
- xiv. Redundancja środków przetwarzania informacji
- xv. Rejestrowanie działań
- xvi. Działania monitorujące
- xvii. Synchronizacja zegarów
- xxviii. Użycie uprzywilejowanych programów narzędziowych
- xix. Instalacja oprogramowania w systemach operacyjnych
- xx. Zabezpieczenia sieci
- xxi. Bezpieczeństwo usług sieciowych
- xxii. Rozdzielenie sieci
- xxiii. Filtrowanie stron internetowych
- xxiv. Użycie kryptografii
- xxv. Bezpieczeństwo prac rozwojowych
- xxvi. Wymagania bezpieczeństwa aplikacji
- xxvii. Zasady projektowania bezpiecznych systemów
- xxviii. Bezpieczne programowanie
- xxix. Testowanie bezpieczeństwa w fazie rozwoju i akceptacja
- xxx. Outsourcing prac rozwojowych
- xxxi. Rozdzielenie środowisk deweloperskich, testowych i produkcyjnych
- xxxii. Zarządzanie zmianami
- xxxiii. Ochrona danych testowych
- xxxiv. Ochrona systemów informatycznych podczas testów audytowych

4. W toku wdrażania dokumentacji nie mogą zostać przekazane Zamawiającemu puste druki (wzorce) dokumentów, jednakże ich wdrożenie powinno opierać się na wypełnieniu wdrażanej dokumentacji zgodnie ze stanem przypadającym na okres wdrożenia. Zamawiający deklaruje przekazywanie niezbędnych danych Wykonawcy, jednakże Wykonawca powinien odpowiednio wdrożyć zapisy do dokumentów przekazywanych Zamawiającemu.
5. W toku wdrażania dokumentacji u Zamawiającego Wykonawca zobowiązany jest do zapewnienia dostępności osób wskazanych w wykazie osób, w ramach prowadzonego postępowania, w siedzibie Zamawiającego przez okres minimum 5 godzin.
6. Zamawiający wymaga, żeby zapisy dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji odnosiły się do wymagań norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005. Dokumentacja powinna być przygotowana w oparciu o wytyczne wynikające z norm ISO 31000 w zakresie zarządzania ryzykiem oraz zarządzania ciągłością działania PN-EN ISO 22301. Zamawiający dokona weryfikacji zgodności na etapie odbioru dokumentacji. W przypadku wykrycia niezgodności Wykonawca będzie zobowiązany do wprowadzenia poprawek zgodnych z wolą Zamawiającego, przy czym wprowadzane poprawki będą realizowane w ramach zawartej umowy, bez dodatkowego wynagrodzenia.
7. Wykonawca w ramach realizacji umowy zapewni przez cały okres realizacji umowy wsparcie Pełnomocnika ds. SZBI, który będzie dostępny zdalnie na żądanie pracowników Zamawiającego w zakresie prawidłowego wykorzystywania dokumentacji systemu zarządzania bezpieczeństwem informacji. Możliwość wsparcia Pełnomocnika ds. SZBI powinna zostać zapewniona w ciągu 5 dni roboczych od zgłoszenia potrzeby pracowników Zamawiającego.

## **6. Opracowanie wraz z wdrożeniem dokumentacji SZBI dla Szkoły Podstawowej im. Tadeusza Kościuszki w Ściechowie.**

W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do aktualizacji dokumentacji z zakresu bezpieczeństwa informacji posiadanej przez Zamawiającego oraz opracowania i wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Szczegółowy opis realizowanych w ramach zamówienia czynności związanych z wdrożeniem dokumentacji systemu zarządzania bezpieczeństwem informacji:

1. W ramach wykonywanych prac Wykonawca zapewni zgodność dokumentacji z poniższymi wymaganiami:
  - a. 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;
  - b. ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa wraz z nowelizacjami ustawy, które zostaną dokonane w czasie realizacji zamówienia;
  - c. 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);

- d. wymagania norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005 i w oparciu o główne założenia norm ISO 31000 w zakresie zarządzania ryzykiem oraz PN-EN ISO 22301 w zakresie ciągłości działania;
  - e. wymagania regulaminu konkursu grantowego oraz umowy o powierzenie grantu zawartej w ramach projektu „Cyberbezpieczny Samorząd”.
2. Wdrażany System Zarządzania Bezpieczeństwem Informacji powinien składać się z obszarów regulujących następujące obszary:
- a. zarządzanie aktywami,
  - b. zarządzanie ryzykiem,
  - c. zapewnienie bezpieczeństwa systemów informatycznych oraz ich rozwoju,
  - d. zapewnienie bezpieczeństwa fizycznego,
  - e. kontrola dostępu do oprogramowania i infrastruktury sieciowej,
  - f. klasyfikacja informacji oraz nadzoru nad dokumentacją,
  - g. zapewnienie bezpieczeństwa zasobów ludzkich,
  - h. wykonywanie kopii zapasowych,
  - i. stosowanie kryptografii,
  - j. obsługa incydentów i realizacja działań korygujących,
  - k. prowadzenie wewnętrznych audytów bezpieczeństwa,
  - l. prowadzenie przeglądów zarządzania,
  - m. zapewnienie ciągłości działania i przywracania normalnej działalności po wystąpieniu zakłóceń,
  - n. zapewnienie bezpieczeństwa łańcucha dostaw,
  - o. postępowanie z podatnościami systemów i sieci,
  - p. Deklaracja stosowania (w oparciu o załącznik A do normy ISO/IEC 27001:2022).
3. W ramach wdrażania Systemu Zarządzania Bezpieczeństwem Informacji powinny zostać uregulowane zabezpieczenia określone w załączniku A do normy ISO/IEC 27001:2022:
- a. Zabezpieczenia organizacyjne
    - i. Polityki bezpieczeństwa informacji
    - ii. Role i obowiązki w zakresie bezpieczeństwa informacji
    - iii. Rozdzielenie obowiązków
    - iv. Odpowiedzialność kierownictwa
    - v. Kontakty z organami władzy
    - vi. Kontakty z grupami zainteresowanych specjalistów
    - vii. Informacja o zagrożeniach
    - viii. Bezpieczeństwo informacji w zarządzaniu projektami
    - ix. Inwentaryzacja informacji i innych powiązanych aktywów
    - x. Akceptowalne użycie informacji i innych powiązanych aktywów
    - xi. Zwrot aktywów
    - xii. Klasyfikacja informacji
    - xiii. Oznaczanie informacji
    - xiv. Przesyłanie informacji
    - xv. Kontrola dostępu

- xvi. Zarządzanie tożsamością (prawami dostępu)
- xvii. Informacje uwierzytelniające
- xviii. Prawa dostępu
- xix. Bezpieczeństwo informacji w relacjach z dostawcami
- xx. Uwzględnienie bezpieczeństwa informacji w umowach z dostawcami
- xxi. Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw technologii informacyjno-komunikacyjnych (ICT)
- xxii. Monitorowanie, przegląd i zarządzanie zmianą usług świadczonych przez dostawców
- xxiii. Bezpieczeństwo informacji w usłudze chmury
- xxiv. Planowanie i przygotowywanie się do zarządzania incydentami bezpieczeństwa informacji
- xxv. Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji
- xxvi. Reagowanie na incydenty bezpieczeństwa informacji
- xxvii. Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji
- xxviii. Gromadzenie materiałów dowodowych
- xxix. Bezpieczeństwo informacji podczas zakłóceń
- xxx. Gotowość teleinformatyczna do zapewnienia ciągłości działania
- xxxi. Wymogi prawne, ustawowe, regulacyjne i umowne
- xxxii. Prawa własności intelektualnej
- xxxiii. Ochrona zapisów
- xxxiv. Prywatność i ochrona danych osobowych (PII)
- xxxv. Niezależny przegląd bezpieczeństwa informacji
- xxxvi. Zgodność z politykami, zasadami i standardami bezpieczeństwa informacji
- xxxvii. Dokumentowanie procedur operacyjnych

b. Zabezpieczenia związane z ludźmi

- i. Postępowanie sprawdzające
- ii. Warunki zatrudnienia
- iii. Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
- iv. Postępowania dyscyplinarne
- v. Zakończenie zatrudnienia lub zmiana zakresu obowiązków
- vi. Umowy o zachowaniu poufności
- vii. Praca zdalna
- viii. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji

c. Zabezpieczenia fizyczne

- i. Fizyczna granica obszaru bezpiecznego
- ii. Zabezpieczenie fizycznych wejść
- iii. Zabezpieczenie biur, pomieszczeń i obiektów
- iv. Monitorowanie bezpieczeństwa fizycznego
- v. Ochrona przed zagrożeniami fizycznymi i środowiskowymi

- vi. Praca w obszarach bezpiecznych
- vii. Polityka czystego biurka i czystego ekranu
- viii. Lokalizacja i ochrona sprzętu
- ix. Bezpieczeństwo sprzętu i aktywów poza siedzibą
- x. Zarządzanie nośnikami danych
- xi. Systemy wspomagające
- xii. Bezpieczeństwo okablowania
- xiii. Konserwacja sprzętu
- xiv. Bezpieczne zbywanie lub przekazywanie do ponownego użycia

d. Zabezpieczenia technologiczne

- i. Urządzenia końcowe użytkowników
- ii. Uprzywilejowane prawa dostępu
- iii. Ograniczenie dostępu do informacji
- iv. Dostęp do kodów źródłowych
- v. Bezpieczne uwierzytelnienie
- vi. Zarządzanie pojemnością
- vii. Zabezpieczenie przed szkodliwym oprogramowaniem
- viii. Zarządzanie podatnościami technicznymi
- ix. Zarządzanie konfiguracją
- x. Usuwanie informacji
- xi. Maskowanie danych
- xii. Zapobieganie wyciekom danych
- xiii. Zapasowe kopie bezpieczeństwa
- xiv. Redundancja środków przetwarzania informacji
- xv. Rejestrowanie działań
- xvi. Działania monitorujące
- xvii. Synchronizacja zegarów
- xviii. Użycie uprzywilejowanych programów narzędziowych
- xix. Instalacja oprogramowania w systemach operacyjnych
- xx. Zabezpieczenia sieci
- xxi. Bezpieczeństwo usług sieciowych
- xxii. Rozdzielenie sieci
- xxiii. Filtrowanie stron internetowych
- xxiv. Użycie kryptografii
- xxv. Bezpieczeństwo prac rozwojowych
- xxvi. Wymagania bezpieczeństwa aplikacji
- xxvii. Zasady projektowania bezpiecznych systemów
- xxviii. Bezpieczne programowanie
- xxix. Testowanie bezpieczeństwa w fazie rozwoju i akceptacja
- xxx. Outsourcing prac rozwojowych

- xxxi. Rozdzielenie środowisk deweloperskich, testowych i produkcyjnych
  - xxxii. Zarządzanie zmianami
  - xxxiii. Ochrona danych testowych
  - xxxiv. Ochrona systemów informatycznych podczas testów audytowych
4. W toku wdrażania dokumentacji nie mogą zostać przekazane Zamawiającemu puste druki (wzorce) dokumentów, jednakże ich wdrożenie powinno opierać się na wypełnieniu wdrażanej dokumentacji zgodnie ze stanem przypadającym na okres wdrożenia. Zamawiający deklaruje przekazywanie niezbędnych danych Wykonawcy, jednakże Wykonawca powinien odpowiednio wdrożyć zapisy do dokumentów przekazywanych Zamawiającemu.
  5. W toku wdrażania dokumentacji u Zamawiającego Wykonawca zobowiązany jest do zapewnienia dostępności osób wskazanych w wykazie osób, w ramach prowadzonego postępowania, w siedzibie Zamawiającego przez okres minimum 5 godzin.
  6. Zamawiający wymaga, żeby zapisy dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji odnosiły się do wymagań norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005. Dokumentacja powinna być przygotowana w oparciu o wytyczne wynikające z norm ISO 31000 w zakresie zarządzania ryzykiem oraz zarządzania ciągłością działania PN-EN ISO 22301. Zamawiający dokona weryfikacji zgodności na etapie odbioru dokumentacji. W przypadku wykrycia niezgodności Wykonawca będzie zobowiązany do wprowadzenia poprawek zgodnych z wolą Zamawiającego, przy czym wprowadzane poprawki będą realizowane w ramach zawartej umowy, bez dodatkowego wynagrodzenia.
  7. Wykonawca w ramach realizacji umowy zapewni przez cały okres realizacji umowy wsparcie Pełnomocnika ds. SZBI, który będzie dostępny zdalnie na żądanie pracowników Zamawiającego w zakresie prawidłowego wykorzystywania dokumentacji systemu zarządzania bezpieczeństwem informacji. Możliwość wsparcia Pełnomocnika ds. SZBI powinna zostać zapewniona w ciągu 5 dni roboczych od zgłoszenia potrzeby pracowników Zamawiającego.

## **7. Opracowanie wraz z wdrożeniem dokumentacji SZBI dla Przedszkola w Baczynie i Przedszkola Gminnego w Lubiszynie.**

W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do aktualizacji dokumentacji z zakresu bezpieczeństwa informacji posiadanej przez Zamawiającego oraz opracowania i wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Szczegółowy opis realizowanych w ramach zamówienia czynności związanych z wdrożeniem dokumentacji systemu zarządzania bezpieczeństwem informacji:

1. W ramach wykonywanych prac Wykonawca zapewni zgodność dokumentacji z poniższymi wymaganiami:
  - a. 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;
  - b. ustawa z dnia z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa wraz z nowelizacjami ustawy, które zostaną dokonane w czasie realizacji zamówienia;

- c. 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);
  - d. wymagania norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005 i w oparciu o główne założenia norm ISO 31000 w zakresie zarządzania ryzykiem oraz PN-EN ISO 22301 w zakresie ciągłości działania;
  - e. wymagania regulaminu konkursu grantowego oraz umowy o powierzenie grantu zawartej w ramach projektu „Cyberbezpieczny Samorząd”.
2. Wdrażany System Zarządzania Bezpieczeństwem Informacji powinien składać się z obszarów regulujących następujące obszary:
- a. zarządzanie aktywami,
  - b. zarządzanie ryzykiem,
  - c. zapewnienie bezpieczeństwa systemów informatycznych oraz ich rozwoju,
  - d. zapewnienie bezpieczeństwa fizycznego,
  - e. kontrola dostępu do oprogramowania i infrastruktury sieciowej,
  - f. klasyfikacja informacji oraz nadzoru nad dokumentacją,
  - g. zapewnienie bezpieczeństwa zasobów ludzkich,
  - h. wykonywanie kopii zapasowych,
  - i. stosowanie kryptografii,
  - j. obsługa incydentów i realizacja działań korygujących,
  - k. prowadzenie wewnętrznych audytów bezpieczeństwa,
  - l. prowadzenie przeglądów zarządzania,
  - m. zapewnienie ciągłości działania i przywracania normalnej działalności po wystąpieniu zakłóceń,
  - n. zapewnienie bezpieczeństwa łańcucha dostaw,
  - o. postępowanie z podatnościami systemów i sieci,
  - p. Deklaracja stosowania (w oparciu o załącznik A do normy ISO/IEC 27001:2022).
3. W ramach wdrażania Systemu Zarządzania Bezpieczeństwem Informacji powinny zostać uregulowane zabezpieczenia określone w załączniku A do normy ISO/IEC 27001:2022:
- a. Zabezpieczenia organizacyjne
    - i. Polityki bezpieczeństwa informacji
    - ii. Role i obowiązki w zakresie bezpieczeństwa informacji
    - iii. Rozdzielenie obowiązków
    - iv. Odpowiedzialność kierownictwa
    - v. Kontakty z organami władzy
    - vi. Kontakty z grupami zainteresowanych specjalistów
    - vii. Informacja o zagrożeniach
    - viii. Bezpieczeństwo informacji w zarządzaniu projektami
    - ix. Inwentaryzacja informacji i innych powiązanych aktywów
    - x. Akceptowalne użycie informacji i innych powiązanych aktywów
    - xi. Zwrot aktywów

- xii. Klasyfikacja informacji
  - xiii. Oznaczanie informacji
  - xiv. Przesyłanie informacji
  - xv. Kontrola dostępu
  - xvi. Zarządzanie tożsamością (prawami dostępu)
  - xvii. Informacje uwierzytelniające
  - xviii. Prawa dostępu
  - xix. Bezpieczeństwo informacji w relacjach z dostawcami
  - xx. Uwzględnienie bezpieczeństwa informacji w umowach z dostawcami
  - xxi. Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw technologii informacyjno-komunikacyjnych (ICT)
  - xxii. Monitorowanie, przegląd i zarządzanie zmianą usług świadczonych przez dostawców
  - xxiii. Bezpieczeństwo informacji w usłudze chmury
  - xxiv. Planowanie i przygotowywanie się do zarządzania incydentami bezpieczeństwa informacji
  - xxv. Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji
  - xxvi. Reagowanie na incydenty bezpieczeństwa informacji
  - xxvii. Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji
  - xxviii. Gromadzenie materiałów dowodowych
  - xxix. Bezpieczeństwo informacji podczas zakłóceń
  - xxx. Gotowość teleinformatyczna do zapewnienia ciągłości działania
  - xxxi. Wymogi prawne, ustawowe, regulacyjne i umowne
  - xxxii. Prawa własności intelektualnej
  - xxxiii. Ochrona zapisów
  - xxxiv. Prywatność i ochrona danych osobowych (PII)
  - xxxv. Niezależny przegląd bezpieczeństwa informacji
  - xxxvi. Zgodność z politykami, zasadami i standardami bezpieczeństwa informacji
  - xxxvii. Dokumentowanie procedur operacyjnych
- b. Zabezpieczenia związane z ludźmi
- i. Postępowanie sprawdzające
  - ii. Warunki zatrudnienia
  - iii. Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
  - iv. Postępowania dyscyplinarne
  - v. Zakończenie zatrudnienia lub zmiana zakresu obowiązków
  - vi. Umowy o zachowaniu poufności
  - vii. Praca zdalna
  - viii. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji
- c. Zabezpieczenia fizyczne
- i. Fizyczna granica obszaru bezpiecznego



- ii. Zabezpieczenie fizycznych wejść
- iii. Zabezpieczenie biur, pomieszczeń i obiektów
- iv. Monitorowanie bezpieczeństwa fizycznego
- v. Ochrona przed zagrożeniami fizycznymi i środowiskowymi
- vi. Praca w obszarach bezpiecznych
- vii. Polityka czystego biurka i czystego ekranu
- viii. Lokalizacja i ochrona sprzętu
- ix. Bezpieczeństwo sprzętu i aktywów poza siedzibą
- x. Zarządzanie nośnikami danych
- xi. Systemy wspomagające
- xii. Bezpieczeństwo okablowania
- xiii. Konserwacja sprzętu
- xiv. Bezpieczne zbywanie lub przekazywanie do ponownego użycia

d. Zabezpieczenia technologiczne

- i. Urządzenia końcowe użytkowników
- ii. Uprzywilejowane prawa dostępu
- iii. Ograniczenie dostępu do informacji
- iv. Dostęp do kodów źródłowych
- v. Bezpieczne uwierzytelnienie
- vi. Zarządzanie pojemnością
- vii. Zabezpieczenie przed szkodliwym oprogramowaniem
- viii. Zarządzanie podatnościami technicznymi
- ix. Zarządzanie konfiguracją
- x. Usuwanie informacji
- xi. Maskowanie danych
- xii. Zapobieganie wyciekom danych
- xiii. Zapasowe kopie bezpieczeństwa
- xiv. Redundancja środków przetwarzania informacji
- xv. Rejestrowanie działań
- xvi. Działania monitorujące
- xvii. Synchronizacja zegarów
- xviii. Użycie uprzywilejowanych programów narzędziowych
- xix. Instalacja oprogramowania w systemach operacyjnych
- xx. Zabezpieczenia sieci
- xxi. Bezpieczeństwo usług sieciowych
- xxii. Rozdzielenie sieci
- xxiii. Filtrowanie stron internetowych
- xxiv. Użycie kryptografii
- xxv. Bezpieczeństwo prac rozwojowych
- xxvi. Wymagania bezpieczeństwa aplikacji



- xxvii. Zasady projektowania bezpiecznych systemów
  - xxviii. Bezpieczne programowanie
  - xxix. Testowanie bezpieczeństwa w fazie rozwoju i akceptacja
  - xxx. Outsourcing prac rozwojowych
  - xxxi. Rozdzielenie środowisk deweloperskich, testowych i produkcyjnych
  - xxxii. Zarządzanie zmianami
  - xxxiii. Ochrona danych testowych
  - xxxiv. Ochrona systemów informatycznych podczas testów audytowych
4. W toku wdrażania dokumentacji nie mogą zostać przekazane Zamawiającemu puste druki (wzorce) dokumentów, jednakże ich wdrożenie powinno opierać się na wypełnieniu wdrażanej dokumentacji zgodnie ze stanem przypadającym na okres wdrożenia. Zamawiający deklaruje przekazywanie niezbędnych danych Wykonawcy, jednakże Wykonawca powinien odpowiednio wdrożyć zapisy do dokumentów przekazywanych Zamawiającemu.
5. W toku wdrażania dokumentacji u Zamawiającego Wykonawca zobowiązany jest do zapewnienia dostępności osób wskazanych w wykazie osób, w ramach prowadzonego postępowania, w siedzibie Zamawiającego przez okres minimum 5 godzin.
6. Zamawiający wymaga, żeby zapisy dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji odnosiły się do wymagań norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005. Dokumentacja powinna być przygotowana w oparciu o wytyczne wynikające z norm ISO 31000 w zakresie zarządzania ryzykiem oraz zarządzania ciągłością działania PN-EN ISO 22301. Zamawiający dokona weryfikacji zgodności na etapie odbioru dokumentacji. W przypadku wykrycia niezgodności Wykonawca będzie zobowiązany do wprowadzenia poprawek zgodnych z wolą Zamawiającego, przy czym wprowadzane poprawki będą realizowane w ramach zawartej umowy, bez dodatkowego wynagrodzenia.
7. Wykonawca w ramach realizacji umowy zapewni przez cały okres realizacji umowy wsparcie Pełnomocnika ds. SZBI, który będzie dostępny zdalnie na żądanie pracowników Zamawiającego w zakresie prawidłowego wykorzystywania dokumentacji systemu zarządzania bezpieczeństwem informacji. Możliwość wsparcia Pełnomocnika ds. SZBI powinna zostać zapewniona w ciągu 5 dni roboczych od zgłoszenia potrzeby pracowników Zamawiającego.

## **8. Opracowanie wraz z wdrożeniem dokumentacji SZBI dla Zakładu Usług Komunalnych w Lubiszynie.**

W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do aktualizacji dokumentacji z zakresu bezpieczeństwa informacji posiadanej przez Zamawiającego oraz opracowania i wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Szczegółowy opis realizowanych w ramach zamówienia czynności związanych z wdrożeniem dokumentacji systemu zarządzania bezpieczeństwem informacji:

1. W ramach wykonywanych prac Wykonawca zapewni zgodność dokumentacji z poniższymi wymaganiami:

- a. 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;
  - b. ustawa z dnia z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa wraz z nowelizacjami ustawy, które zostaną dokonane w czasie realizacji zamówienia;
  - c. 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);
  - d. wymagania norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005 i w oparciu o główne założenia norm ISO 31000 w zakresie zarządzania ryzykiem oraz PN-EN ISO 22301 w zakresie ciągłości działania;
  - e. wymagania regulaminu konkursu grantowego oraz umowy o powierzenie grantu zawartej w ramach projektu „Cyberbezpieczny Samorząd”.
2. Wdrażany System Zarządzania Bezpieczeństwem Informacji powinien składać się z obszarów regulujących następujące obszary:
  - a. zarządzanie aktywami,
  - b. zarządzanie ryzykiem,
  - c. zapewnienie bezpieczeństwa systemów informatycznych oraz ich rozwoju,
  - d. zapewnienie bezpieczeństwa fizycznego,
  - e. kontrola dostępu do oprogramowania i infrastruktury sieciowej,
  - f. klasyfikacja informacji oraz nadzoru nad dokumentacją,
  - g. zapewnienie bezpieczeństwa zasobów ludzkich,
  - h. wykonywanie kopii zapasowych,
  - i. stosowanie kryptografii,
  - j. obsługa incydentów i realizacja działań korygujących,
  - k. prowadzenie wewnętrznych audytów bezpieczeństwa,
  - l. prowadzenie przeglądów zarządzania,
  - m. zapewnienie ciągłości działania i przywracania normalnej działalności po wystąpieniu zakłóceń,
  - n. zapewnienie bezpieczeństwa łańcucha dostaw,
  - o. postępowanie z podatnościami systemów i sieci,
  - p. Deklaracja stosowania (w oparciu o załącznik A do normy ISO/IEC 27001:2022).
3. W ramach wdrażania Systemu Zarządzania Bezpieczeństwem Informacji powinny zostać uregulowane zabezpieczenia określone w załączniku A do normy ISO/IEC 27001:2022:
  - a. Zabezpieczenia organizacyjne
    - i. Polityki bezpieczeństwa informacji
    - ii. Role i obowiązki w zakresie bezpieczeństwa informacji
    - iii. Rozdzielenie obowiązków
    - iv. Odpowiedzialność kierownictwa
    - v. Kontakty z organami władzy
    - vi. Kontakty z grupami zainteresowanych specjalistów

- vii. Informacja o zagrożeniach
- viii. Bezpieczeństwo informacji w zarządzaniu projektami
- ix. Inwentaryzacja informacji i innych powiązanych aktywów
- x. Akceptowalne użycie informacji i innych powiązanych aktywów
- xi. Zwrot aktywów
- xii. Klasyfikacja informacji
- xiii. Oznaczanie informacji
- xiv. Przesyłanie informacji
- xv. Kontrola dostępu
- xvi. Zarządzanie tożsamością (prawami dostępu)
- xvii. Informacje uwierzytelniające
- xviii. Prawa dostępu
- xix. Bezpieczeństwo informacji w relacjach z dostawcami
- xx. Uwzględnienie bezpieczeństwa informacji w umowach z dostawcami
- xxi. Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw technologii informacyjno-komunikacyjnych (ICT)
- xxii. Monitorowanie, przegląd i zarządzanie zmianą usług świadczonych przez dostawców
- xxiii. Bezpieczeństwo informacji w usłudze chmury
- xxiv. Planowanie i przygotowywanie się do zarządzania incydentami bezpieczeństwa informacji
- xxv. Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji
- xxvi. Reagowanie na incydenty bezpieczeństwa informacji
- xxvii. Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji
- xxviii. Gromadzenie materiałów dowodowych
- xxix. Bezpieczeństwo informacji podczas zakłóceń
- xxx. Gotowość teleinformatyczna do zapewnienia ciągłości działania
- xxxi. Wymogi prawne, ustawowe, regulacyjne i umowne
- xxxii. Prawa własności intelektualnej
- xxxiii. Ochrona zapisów
- xxxiv. Prywatność i ochrona danych osobowych (PII)
- xxxv. Niezależny przegląd bezpieczeństwa informacji
- xxxvi. Zgodność z politykami, zasadami i standardami bezpieczeństwa informacji
- xxxvii. Dokumentowanie procedur operacyjnych

b. Zabezpieczenia związane z ludźmi

- i. Postępowanie sprawdzające
- ii. Warunki zatrudnienia
- iii. Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
- iv. Postępowania dyscyplinarne
- v. Zakończenie zatrudnienia lub zmiana zakresu obowiązków
- vi. Umowy o zachowaniu poufności

- vii. Praca zdalna
- viii. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji

c. Zabezpieczenia fizyczne

- i. Fizyczna granica obszaru bezpiecznego
- ii. Zabezpieczenie fizycznych wejść
- iii. Zabezpieczenie biur, pomieszczeń i obiektów
- iv. Monitorowanie bezpieczeństwa fizycznego
- v. Ochrona przed zagrożeniami fizycznymi i środowiskowymi
- vi. Praca w obszarach bezpiecznych
- vii. Polityka czystego biurka i czystego ekranu
- viii. Lokalizacja i ochrona sprzętu
- ix. Bezpieczeństwo sprzętu i aktywów poza siedzibą
- x. Zarządzanie nośnikami danych
- xi. Systemy wspomagające
- xii. Bezpieczeństwo okablowania
- xiii. Konserwacja sprzętu
- xiv. Bezpieczne zbywanie lub przekazywanie do ponownego użycia

d. Zabezpieczenia technologiczne

- i. Urządzenia końcowe użytkowników
- ii. Uprzywilejowane prawa dostępu
- iii. Ograniczenie dostępu do informacji
- iv. Dostęp do kodów źródłowych
- v. Bezpieczne uwierzytelnienie
- vi. Zarządzanie pojemnością
- vii. Zabezpieczenie przed szkodliwym oprogramowaniem
- viii. Zarządzanie podatnościami technicznymi
- ix. Zarządzanie konfiguracją
- x. Usuwanie informacji
- xi. Maskowanie danych
- xii. Zapobieganie wyciekom danych
- xiii. Zapasowe kopie bezpieczeństwa
- xiv. Redundancja środków przetwarzania informacji
- xv. Rejestrowanie działań
- xvi. Działania monitorujące
- xvii. Synchronizacja zegarów
- xviii. Użycie uprzywilejowanych programów narzędziowych
- xix. Instalacja oprogramowania w systemach operacyjnych
- xx. Zabezpieczenia sieci
- xxi. Bezpieczeństwo usług sieciowych

- xxii. Rozdzielenie sieci
  - xxiii. Filtrowanie stron internetowych
  - xxiv. Użycie kryptografii
  - xxv. Bezpieczeństwo prac rozwojowych
  - xxvi. Wymagania bezpieczeństwa aplikacji
  - xxvii. Zasady projektowania bezpiecznych systemów
  - xxviii. Bezpieczne programowanie
  - xxix. Testowanie bezpieczeństwa w fazie rozwoju i akceptacja
  - xxx. Outsourcing prac rozwojowych
  - xxxi. Rozdzielenie środowisk deweloperskich, testowych i produkcyjnych
  - xxxii. Zarządzanie zmianami
  - xxxiii. Ochrona danych testowych
  - xxxiv. Ochrona systemów informatycznych podczas testów audytowych
4. W toku wdrażania dokumentacji nie mogą zostać przekazane Zamawiającemu puste druki (wzorce) dokumentów, jednakże ich wdrożenie powinno opierać się na wypełnieniu wdrażanej dokumentacji zgodnie ze stanem przypadającym na okres wdrożenia. Zamawiający deklaruje przekazywanie niezbędnych danych Wykonawcy, jednakże Wykonawca powinien odpowiednio wdrożyć zapisy do dokumentów przekazywanych Zamawiającemu.
5. W toku wdrażania dokumentacji u Zamawiającego Wykonawca zobowiązany jest do zapewnienia dostępności osób wskazanych w wykazie osób, w ramach prowadzonego postępowania, w siedzibie Zamawiającego przez okres minimum 5 godzin.
6. Zamawiający wymaga, żeby zapisy dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji odnosiły się do wymagań norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005. Dokumentacja powinna być przygotowana w oparciu o wytyczne wynikające z norm ISO 31000 w zakresie zarządzania ryzykiem oraz zarządzania ciągłością działania PN-EN ISO 22301. Zamawiający dokona weryfikacji zgodności na etapie odbioru dokumentacji. W przypadku wykrycia niezgodności Wykonawca będzie zobowiązany do wprowadzenia poprawek zgodnych z wolą Zamawiającego, przy czym wprowadzane poprawki będą realizowane w ramach zawartej umowy, bez dodatkowego wynagrodzenia.
7. Wykonawca w ramach realizacji umowy zapewni przez cały okres realizacji umowy wsparcie Pełnomocnika ds. SZBI, który będzie dostępny zdalnie na żądanie pracowników Zamawiającego w zakresie prawidłowego wykorzystywania dokumentacji systemu zarządzania bezpieczeństwem informacji. Możliwość wsparcia Pełnomocnika ds. SZBI powinna zostać zapewniona w ciągu 5 dni roboczych od zgłoszenia potrzeby pracowników Zamawiającego.

## 9. Szkolenie z zakresu cyberbezpieczeństwa dla pracowników oświaty.

W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do:

1. Wykonania analizy wiedzy pracowników oraz realizowanych działań w ramach przestrzegania zasad bezpieczeństwa informacji i wytycznych w zakresie cyberbezpieczeństwa poprzez realizację zdalnego testu socjotechnicznego.

2. Przygotowanie i przeprowadzenie szkoleń dla pracowników z zakresu cyberbezpieczeństwa (szkolenia stacjonarne dla liczby osób wskazanych przez Zamawiającego w minimum czterech grupach szkoleniowych, w budynku na terenie Gminy Lubiszyn, w terminie do 30 kwietnia 2026 roku, czas trwania jednej grupy szkoleniowej to 3 godziny, realizacja minimum w dwa dni robocze).

Szczegółowy opis realizowanych w ramach zamówienia czynności związanych z wykonaniem analizy wiedzy pracowników oraz realizowanych działań w ramach przestrzegania zasad bezpieczeństwa informacji i wytycznych w zakresie cyberbezpieczeństwa poprzez realizację zdalnego testu socjotechnicznego (punkt numer 1):

1. W ramach wykonywanych prac Wykonawca przeprowadzi kompleksową weryfikację wiedzy z zakresu przestrzegania zasad bezpieczeństwa informacji poprzez wykonanie testu socjotechnicznego.
2. Wykonawca wspólnie z Zamawiającym ustali szczegółowy scenariusz testu socjotechnicznego, który będzie odpowiadał na aktualne problemy związane z pracą Zamawiającego lub sytuacją społeczno – gospodarczą.
3. Wykonawca przeprowadzi test socjotechniczny z dedykowanego adresu mailowego opartego na specjalnie założonej stronie internetowej pozwalającej na uwiarygodnienie wiadomości.
4. Wykonawca zaprojektuje minimum jeden szablon wiadomości mailowej, która będzie wysyłana z dedykowanej strony internetowej.
5. Zamawiający przekaze Wykonawcy adresy mailowe pracowników objętych testem.
6. Wykonawca przeprowadzi wysyłkę wiadomości mailowych, przyjmując odpowiedni podział pracowników.
7. W trakcie realizacji testu Wykonawca będzie odpowiedzialny za monitorowanie reakcji pracowników, analizowanie odpowiedzi i interakcji odbiorców z wysłanymi wiadomościami, a także wprowadzanie zmian w realizowanej kampanii, w celu zapewnienia efektywności testu.
8. Wykonawca przeanalizuje wyniki testów oraz na tej podstawie opracuje raport, który zostanie przekazany Zamawiającemu, a następnie będzie stanowił podstawę do odpowiedniej analizy tematyki szkoleń i zostanie przedstawiony pracownikom podczas szkoleń.

Szczegółowy opis realizowanych w ramach zamówienia czynności związanych z przygotowaniem i przeprowadzeniem szkoleń dla pracowników z zakresu cyberbezpieczeństwa (punkt numer 2):

1. W ramach wykonywanych prac materiał szkoleniowy zaprezentowany przez Wykonawcę będzie odwoływał się do poniższych wymagań prawnych:
  - a. 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 (RODO);
  - b. ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
  - c. ustawy z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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;
  - d. rozporządzenia Rady Ministrów z dnia 21 maja 2014 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;

- e. ustawy z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami;
  - f. ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych;
  - g. wytycznych CSIRT NASK.
2. Przeprowadzanie szkolenie pracowników będzie odnosiło się do zasad cyberbezpieczeństwa w ramach wykonywanej pracy zapewniające bezpieczeństwo zasobów jednostki.
3. W toku realizacji szkoleń Wykonawca jest zobowiązany do przedstawienia następujących obszarów:
- a. Czym jest phishing?
  - b. Czym jest ransomware?
  - c. Socjotechnika jako podstawowe narzędzie sprawców ataków.
  - d. Zasady bezpiecznego korzystania z Internetu;
  - e. Zasady bezpiecznego korzystania z portali społecznościowych;
  - f. Zasady bezpiecznego korzystania z poczty elektronicznej i zagrożenia z tym związane;
  - g. Zasady bezpiecznego korzystania z haseł;
  - h. Zagrożenia bezpieczeństwa informacji przy korzystaniu z sieci Internet.
    - i. Ataki przez pocztę e-mail
    - ii. Ataki przez strony WWW
    - iii. Bezpieczna praca z przeglądarką internetową
  - i. Bezpieczna praca z programem pocztowym
  - j. Bezpieczne korzystanie z sieci bezprzewodowych (Wi-Fi, Bluetooth).
  - k. Zagrożenia i sposoby zabezpieczania sprzętu mobilnego;
  - l. Korzystanie z menedżera haseł w praktyce;
  - m. Przykłady technik stosowanych przez cyberprzestępców;
  - n. Zasady bezpiecznego realizowania pracy zdalnej.
  - o. Wycieki informacji – mechanizmy i skutki.
  - p. Zarządzanie hasłami – dobre praktyki i narzędzia pomocnicze.
  - q. Psychomanipulacja w sieci – zasady i zastosowania.
  - r. Sfałszowane komunikaty i strony – identyfikacja zagrożeń.
  - s. Ataki głosowe i podszywanie się pod identyfikator dzwoniącego (vishing).
  - t. Deepfake oraz inne zagrożenia wynikające ze stosowania AI w przyszłości.
  - u. Mechanizmy ochronne przed cyberzagrożeniami.
4. Realizowane szkolenia muszą mieć formę stacjonarną.
5. Zamawiający udostępni sale do prowadzenia wszystkich szkoleń stacjonarnych.
6. Wykonawca opracuje i wyda każdemu z uczestników szkoleń imienny certyfikat uczestnictwa w szkoleniach, który będzie oznaczony zgodnie z zasadami wizualizacji programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC).