Załącznik nr 1 do Zapytania ofertowego.

Szczegółowy Opis Przedmiotu Zamówienia

pn. Przeprowadzenie audytu KRI oraz aktualizacja i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w ramach projektu „Cyberbezpieczny Samorząd”

1. Przedmiot zamówienia

1.1. Wymagania ogólne

1. Zamówienie będzie realizowane na rzecz Urzędu Gminy Stary Brus (dalej: UG) oraz Ośrodka Pomocy Społecznej w Starym Brusie (dalej: OPS).
2. Wykonawca będzie zobowiązany do przeprowadzenia w roku 2025 i 2026 audytu systemu zarządzania bezpieczeństwem informacji w związku z zapisami w § 19 ust. 2 pkt 14 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), zwanego dalej „audytem KRI”.
3. Wykonawca jest zobowiązany do przeprowadzenia aktualizacji i wdrożenia kompletnego Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwany: SZBI) w UG i OPS.
4. Zakres audytu systemu bezpieczeństwa informacji każdorazowo obejmie zgodność z kryteriami zawartymi w § 19 ust. 2 ww. rozporządzenia KRI.
5. Raport z audytu KRI zostanie każdorazowo podpisany przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczony do Zamawiającego w formie elektronicznej.
6. Audyt KRI oraz aktualizacja i wdrożenie SZBI muszą zostać przeprowadzone przez:
   1) audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. 2018 poz. 1999) lub
   2) audytora wewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001:2023 lub równoważnej.
7. Wykonawca w trakcie realizacji zamówienia jest zobowiązany do zapoznania się z częściowo wypełnioną ankietą dojrzałości cyberbezpieczeństwa w zakresie wskazanym przez Zamawiającego oraz uwzględnić w ramach aktualizacji i wdrożenia SZBI planowany w ramach realizacji projektu zakres usprawnień SZBI.
8. Wykonawca po wykonaniu ostatniego audytu KRI jest zobowiązany do uzupełnienia ankiety dojrzałości cyberbezpieczeństwa. Ankietę dojrzałości cyberbezpieczeństwa należy wypełnić w oparciu o aktualny na dzień wypełnienia ankiety wzór ankiety opublikowany na stronie: https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad (załącznik nr 6 - Ankieta

Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego i Jednostkach Podległych).

9. Wypełnienie ankiety dojrzałości cyberbezpieczeństwa polegać będzie wypełnieniu przez Wykonawcę kolumn H, I z arkusza „Ankieta" na podstawie zebranych przez Wykonawcę danych. Zamawiający nie dopuszcza pozostawienia pustych pól dla określonych powyżej kolumn, w przypadku jeżeli w polu opisowym nie przewiduje się zmian wówczas należy zamieścić odpowiednią informację. Ankieta dojrzałości cyberbezpieczeństwa zostanie podpisana przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczona do Zamawiającego w formie elektronicznej.
10. Jednostki samorządu terytorialnego oraz ich jednostki podległe, które biorą udział w projekcie „Cyberbezpieczny Samorząd" są zobowiązane do przesłania do NASK raportu z audytu KRI oraz wypełnionej ankiety dojrzałości cyberbezpieczeństwa. Niezwłocznie po ich przekazaniu przez Wykonawcę dokumenty te zostaną przekazane przez Zamawiającego do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK) za pośrednictwem platformy ePUAP. Dane z tej dokumentacji przekazane przez JST do NASK posłużą do opracowania raportu na temat stanu bezpieczeństwa systemów jednostek samorządowych. Wykonawca jest zobowiązany mieć na uwadze także powyżej wskazany cel przeprowadzenia zamówienia i jego przeznaczenie.
11. Wykonawca przy świadczeniu usług jest zobowiązany uwzględnić i zastosować wymagania Dyrektywy 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) oraz akty wykonawcze wydane do niej. W przypadku jeżeli w okresie realizacji zamówienia zostanie przyjęta ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw bądź inne przepisy implementujące Dyrektywę 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) w polski system prawny Wykonawca ma obowiązek uwzględnić wszystkie ich wymagania przy świadczeniu usług objętych niniejszym zamówieniem.
12. Wykonawca zrealizuje zamówienie w oparciu o dokumentację, którą Zamawiający dysponuje niezależnie od realizacji przedmiotu umowy i o wyjaśnienia udzielane przez Zamawiającego. W szczególności realizacja przedmiotu umowy przez Wykonawcę nie może być uwarunkowana wytwarzaniem lub uzupełnianiem dokumentów i opracowań przez Zamawiającego w związku z realizacją przedmiotu umowy, tj. Zamawiający nie może być zobowiązany do wypełniania ankiet, kwestionariuszy, sporządzania notatek itp., a informacje niezbędne Wykonawcy do wykonania przedmiotu umowy mogą być pozyskiwane wyłącznie w postaci materiałów źródłowych i wywiadu bezpośredniego.
13. Zamawiający dopuszcza prowadzenie prac związanych z: analizą dokumentacji, opracowaniem dokumentacji i polityk, opracowania raportów poza siedzibą Zamawiającego. Zamawiający nie dopuszcza prowadzenia instruktaży, konsultacji, audytów, analiz stanu istniejącego i określenie stanu faktycznego zabezpieczeń technicznych w formule zdalnej, tj. w postaci on-line lub innej poza siedzibami UG i OPS.

14. W zakresie usługi aktualizacji i wdrożenia SZBI nie dopuszcza się realizacji więcej niż jednego etapu prac prowadzonych w siedzibach UG i OPS w ciągu jednego dnia roboczego (dotyczy etapów określonych w dalszej części dokumentu).
15. W ramach wynagrodzenia umownego Wykonawca będzie wprowadzał niezbędne zmiany w opracowanej dokumentacji SZBI, o ile okażą się one konieczne w związku ze zmianami regulacji prawnych lub w związku ze zmianami organizacyjnymi lub technicznymi w UG i/lub OPS, jeżeli takie zmiany wystąpią.
16. Zamówienie jest realizowane w ramach projektu pn. „Cyberbezpieczny Samorząd" współfinansowanego ze środków Unii Europejskiej i budżetu państwa w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Priorytetu II Zaawansowane usługi cyfrowe, Działania 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa.

1.2. Zakup usług aktualizacji i wdrożenia SZBI

Celem usługi w ramach działania będzie aktualizacja i wdrożenie procedur systemu zarządzania bezpieczeństwem informacji wdrożonych u Zamawiającego z uwzględnieniem uwarunkowań i specyfiki projektu oraz specyfiki jednostek. Analiza zostanie przeprowadzona z uwzględnieniem wymogów normy ISO/IEC 19011:2002 jako wzorca dobrej praktyki. W efekcie zostanie zaktualizowana także polityka bezpieczeństwa w zakresie ochrony danych osobowych. Usługa obejmuje również aktualizację dokumentów opisujących zbiory danych i ich zgodność z wymogami prawnymi oraz aktualizację dokumentów opisujących miejsca i sposoby przetwarzania danych osobowych.

Na usługę aktualizacji i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji składają się co najmniej:

1. Wykonanie oceny obecnej dostępnej dokumentacji.
2. Określenie stanu faktycznego zabezpieczeń danych w systemach informatycznych poprzez przeprowadzenie audytu zabezpieczeń dostępu do danych oraz przygotowanie raportu zawierającego zalecenia i projekt zmian, z uwzględnieniem wytycznych PN-EN ISO/IEC 27001:2023 i zaleceń norm pokrewnych, a także wymagań prawnych nałożonych na organizację, w tym dotyczących ochrony danych osobowych.
3. Przeprowadzenie instruktażu wprowadzającego dla pracowników w zakresie ochrony informacji, inwentaryzacji aktywów informacyjnych oraz oceny ryzyka.
4. Aktualizacja/opracowanie Polityki Bezpieczeństwa z uwzględnieniem wytycznych normy PN-EN ISO/IEC 27001:2023 jako wzorca dobrej praktyki i zaleceń norm pokrewnych, oraz wymagań prawnych nałożonych na organizację, między innymi dotyczących ochrony danych osobowych w zakresie:
    1) organizacja systemu bezpieczeństwa informacji;
    2) zarządzanie aktywami;
    3) zarządzanie zasobami ludzkimi;
    4) organizacja bezpieczeństwa fizycznego i środowiskowego;
    5) zarządzanie komunikacją i eksploatacją;
    6) rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania;
    7) kontrola dostępu, zarządzania hasłami, stosowania zabezpieczeń kryptograficznych, czystego biurka i czystego ekranu, usuwania i niszczenia informacji, pracy w strefach bezpieczeństwa;
    8) akwizycja, rozwój i utrzymanie systemu;
    9) zarządzanie incydentami związanymi z bezpieczeństwem informacji;

10) zarządzanie ciągłością działania;
11) zarządzania kopiami zapasowymi;
12) zarządzania monitoringiem;
13) zobowiązanie do zachowania poufności, stosowania polityk i procedur SZBI;
14) używania urządzeń komputerowych;
15) metoda szacowania i postępowania z ryzykiem;
16) deklaracja stosowania

5. Wdrożenie Polityki Bezpieczeństwa Informacji. Poprzez wdrożenie należy rozumieć także aktualizację/utworzenie odpowiednich dokumentów po konsultacjach z pracownikami Zamawiającego, zatwierdzenie dokumentacji przez Kierownictwo Zamawiającego oraz przeprowadzenie instruktażu pracowników w zakresie wykonywania obowiązków zgodnie z opracowanym sposobem postępowania w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Ponadto:

1. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje procedury bezpieczeństwa fizycznego obejmujące obowiązek wyznaczania osoby odpowiedzialnej za bezpieczeństwo fizyczne.
2. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje zasady odpowiedzialności za cyberbezpieczeństwo wraz ze wskazaniem obowiązku wyznaczania osoby odpowiedzialnej za cyberbezpieczeństwo.
3. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę szkoleń z zakresu cyberbezpieczeństwa wraz z wprowadzeniem obowiązku regularnego, corocznego prowadzenia szkoleń.
4. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje treść zarządzenia wdrażającego SZBI.
5. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan postępowania z ryzkiem obejmujący systematyczne tworzenie raportów oceny ryzyka w Jednostce oraz konieczność cyklicznego przeglądu tego raportu przez Kierownika JST.
6. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje szczegółowy sposób realizacji celów oraz we współpracy z Zamawiającym przypisze odpowiedzialności za ich realizację.
7. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje procedurę wprowadzającą obowiązek regularnego, corocznego przeglądu PBI jednostki.
8. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę szkoleń obejmującą obowiązek informowania o zmianach w PBI w toku okresowych szkoleń stanowiskowych.
9. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kluczowe aktywa informacyjne Jednostki (zbiory danych/systemy/usługi).
10. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje rejestr ryzyk uwzględniający aktywa Jednostki.
11. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje zagrożenia związane z cyberbezpieczeństwem w ramach procesów zarządczych oraz zarządzania ryzykiem.
12. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan postępowania z ryzkiem związanym z zagrożeniami bezpieczeństwa informacji.
13. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą obowiązek używania do określenia w Jednostce zagrożeń, podatności, prawdopodobieństwa ich wystąpienia i skutków.

14. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą obowiązek identyfikacji i priorytetyzacji odpowiedzi na ryzyka.
15. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą system oceny ryzyka.
16. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem cyberbezpieczeństwa uwzględniającą identyfikowane, ustanawiane i oceniane ryzyka.
17. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania danymi uwzględniającą polityki ich niszczenia, plan backup, plany reagowania i odtwarzania danych.
18. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan zarządzania podatnościami.
19. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania zapisami zdarzeń / logów/ inspekcji.
20. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę użytkowania dostępu do odczytu lub zapisu danych z zewnętrznych nośników danych.
21. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów.
22. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan zarządzania podatnościami uwzględniający obowiązek dokumentowania ryzyka z nimi związanego.
23. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów i ich aktualizacji w obszarze doświadczeń i wniosków z wykrytych i obsłużonych incydentów.
24. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów wraz z obowiązkiem ich aktualizacji.
25. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę planów odtwarzania uwzględniającą obowiązek ich aktualizacji w obszarze doświadczeń i wniosków z prowadzonych procesów odtwarzania.
26. Wykonawca jest zobowiązany dostosować zakres, złożoność i szczegółowość wdrażanego Systemu Zarządzania Bezpieczeństwem Informacji do wielkości, struktury organizacyjnej oraz możliwości kadrowych każdej jednostki objętej wdrożeniem, przy zachowaniu zgodności z wymaganiami prawa oraz podstawowych zasad bezpieczeństwa informacji

Poszczególne etapy realizacji usługi.

Etap I. Audyt zerowy.
1. Określenie stanu spełnienia wymagań prawnych nałożonych na organizację w zakresie ochrony informacji.
2. Sprawdzenie – w charakterze referencyjnym – spełnienia wymagań i zaleceń w ramach standardów PN-EN ISO/IEC 27001:2023 i norm pokrewnych.
3. Inwentaryzacja aktywów informacyjnych i ocena ryzyka.
4. Ocena zabezpieczeń technicznych, organizacyjnych oraz fizycznych.
5. Analiza dokumentacji Polityki Bezpieczeństwa Informacji.
6. Analiza dokumentacji Polityki Bezpieczeństwa Danych Osobowych.

7. Zestaw działań mających na celu określenie stanu faktycznego zabezpieczeń technicznych w systemie informatycznym:
    1) Ocena schematu sieci.
    2) Określenie rodzaju połączeń.
    3) Określenie segmentów sieci.
    4) Przeprowadzenie oceny środowiska informatycznego.
    5) Ocena sposobu identyfikowania i logowania użytkowników.
    6) Analiza zarządzania kontami użytkowników.
    7) Analiza strony www i BIP pod kątem ochrony danych osobowych.
    8) Analiza systemu backupów i archiwizacji danych.
    9) Określenie miejsc redundancji w sieci i systemach informatycznych.
    10) Analiza konfiguracji zabezpieczeń systemów operacyjnych na serwerach.
    11) Analiza konfiguracji zabezpieczeń baz danych.
    12) Określenie bezpieczeństwa aplikacji i serwerów WWW.
    13) Analiza konfiguracji urządzeń sieciowych: switche, routery, IDS, IPS, UTM, firewall.
    14) Ocena zabezpieczeń dostępu do sieci publicznej.
    15) Badanie podatności systemów operacyjnych za pomocą specjalistycznego oprogramowania.
    16) Analiza zabezpieczeń stacji roboczych.
    17) Analiza ochrony danych na komputerach przenośnych.
    18) Badanie zabezpieczeń nośników zewnętrznych.
    19) Sprawdzenie procedur zarządzania ciągłością działania.
8. Opracowanie raportu z audytu zerowego zawierającego analizę bezpieczeństwa i adekwatności zabezpieczeń stosowanych przez Zamawiającego w odniesieniu do sieci i systemów informatycznych oraz rodzaju danych w nich przetwarzanych, z uwzględnieniem obowiązujących przepisów prawa, zasad wiedzy technicznej, wymagań normy PN-EN ISO/IEC 27001:2023 i zaleceń norm pokrewnych.

Etap II. Zastosowanie zabezpieczeń na podstawie zaleceń poaudytowych.

1. Konsultacje przy wdrożeniu zabezpieczeń w infrastrukturze systemu informatycznego;
2. Konsultacje przy wdrożeniu zabezpieczeń organizacyjnych – polityki bezpieczeństwa danych osobowych, zapisów w umowach z dostawcami itp.

Etap III. Planowanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

1. Przeprowadzenie instruktażu dla kadry zarządzającej z zasad bezpieczeństwa informacji.
2. Zakres SZBI:
    1) określenie rodzaju działalności organizacji, jej lokalizacji, rodzajów aktywów i wykorzystywanych technologii;
    2) określenie zasięgu organizacji;
    3) badanie środowiska zewnętrznego, powiązań z innymi organizacjami, systemami oraz dostawcami.
3. Zdefiniowanie wymaganych polityk SZBI:
    1) uwzględnienie rodzaju działalności organizacji, jej lokalizacji, rodzajów aktywów i wykorzystywanych technologii;
    2) analiza wymagań prawnych oraz wymagań wynikających z umów;
    3) uwzględnienie sposobu ustalania celów oraz wyznaczania kierunków działań w ramach systemu.
4. Szacowanie ryzyka:

1) wybór metody szacowania ryzyka;
2) określenie kryteriów akceptowalności ryzyk i identyfikacji akceptowalnych poziomów ryzyk;
3) zdefiniowanie obszarów zabezpieczeń objętych analizą ryzyka.

5. Wybór celów zabezpieczeń:
   1) zdefiniowanie celów zabezpieczeń na podstawie listy zawartej w załączniku A normy PN-EN ISO/IEC 27001:2023;
   2) zdefiniowanie własnych celów zabezpieczania i zabezpieczeń;
   3) uwzględnienie wyników procesu szacowania ryzyka i określenie postępowania z ryzykiem;
   4) określenie środków ochrony.

Etap IV. Inwentaryzacja i szacowanie ryzyka SZBI.

1. Przeprowadzenie instruktaży dla pracowników oraz kadry zarządzającej z metody inwentaryzacji i klasyfikacji aktywów informacyjnych.
2. Wykonanie wraz z pracownikami inwentaryzacji i klasyfikacji aktywów informacyjnych.
3. Zdefiniowanie planu postępowania z ryzykiem:
   1) przeprowadzenie instruktaży dla kadry zarządzającej z wybranej metody oceny ryzyka;
   2) szacowanie i ocena ryzyka – zaktualizowanie wartości ryzyka wynikające z audytu zerowego;
   3) zdefiniowanie planu postępowania z ryzykiem;
   4) określenie planu zarządzania zidentyfikowanymi i oszacowanymi ryzykami;
   5) określenie zadań do realizacji, zdefiniowanie odpowiedzialności i ram czasowych.
4. Opracowanie raportu z oceny ryzyka.

Etap V. Opracowanie niezbędnej dokumentacji SZBI.

1. Opracowanie wspólnie z pracownikami Zamawiającego wymaganych procedur i instrukcji:
   1) opracowanie Polityki Bezpieczeństwa Informacji;
   2) opracowanie Instrukcji Zarządzania Systemem Informatycznym;
   3) opracowanie procedur i instrukcji zgodnie z podejściem proporcjonalnym, odnoszącym się do zaleceń zawartych w normie PN-EN ISO/IEC 27001:2023, przy uwzględnieniu skali i charakteru działalności jednostki;
   4) opracowanie procedur i instrukcji dopasowanych do specyfiki działalności organizacji;
   5) opracowanie Instrukcji postępowania na wypadek wykrycia incydentu naruszenia bezpieczeństwa;
   6) opracowanie procedury audytu wewnętrznego;
   7) opracowanie procedury nadzoru nad dokumentacją;
   8) opracowanie procedury działań korygujących i zapobiegawczych;
   9) opracowanie procedury zachowania ciągłości działania;
   10) opracowanie wraz z pracownikami Zamawiającego planów ciągłości działania.
2. Wykonanie projektu zabezpieczeń - opracowanie projektu zabezpieczeń i konsultacje przy wdrożeniu odpowiednio skutecznych zabezpieczeń zgodnych z celami zabezpieczeń.
3. Opracowanie programu uświadamiania i szkolenia.
4. Przeprowadzenie instruktaży dla pracowników z dokumentacji ochrony informacji.
5. Przeprowadzenie instruktaży dla kadry zarządzającej z dokumentacji ochrony informacji.

Etap VI. Weryfikacja i monitorowanie SZBI.

1. Przeprowadzenie wraz z pracownikami organizacji audytu wewnętrznego.
2. Opracowanie raportu z audytu wewnętrznego.
3. Przeprowadzenie wraz z pracownikami organizacji przeglądu systemu SZBI:
   1) przegląd zagrożeń;
   2) przegląd podatności;
   3) określenie i weryfikacja ryzyk;
   4) weryfikacja planu postępowania z ryzykiem;
   5) sprawdzenie zabezpieczeń i celów zabezpieczeń;
   6) określenie zgodności zakresu SZBI;
   7) weryfikacja zgodności z politykami i celami zabezpieczeń;
   8) przegląd i ocena skuteczności zabezpieczeń;
   9) weryfikacja zgodności wykorzystywania procedur;
   10) weryfikacja zgodności obowiązków i uprawnień w ramach SZBI;
   11) analiza audytów bezpieczeństwa;
   12) weryfikacja dokumentacji i sposobu postępowania z incydentami;
   13) weryfikacja sugestii oraz informacji zwrotnych od zainteresowanych stron;
   14) sprawdzenie aktualności procedur ciągłości działania.
4. Opracowanie raportu z przeglądu.

1.3. Zakup usług przeprowadzenia audytu zgodności KRI

Zakres audytu systemu bezpieczeństwa informacji (zwany na potrzeby przedmiotowego postępowania audytem zgodności KRI, audytem KRI) obejmie zgodność z kryteriami zawartymi w Rozporządzeniu KRI i dotyczyć będzie istniejącej na czas przeprowadzenia audytu dokumentacji systemu zarządzania bezpieczeństwem oraz warunków technicznych bezpieczeństwa informacji (BI) zgodnie z minimalnymi wymaganiami wykonania usługi określonymi poniżej.
Wymagania minimalne wykonania usługi:

1. Przedmiotem zamówienia jest przeprowadzenie audytu dotyczącego spełnienia wymagań 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), zwanym dalej „Rozporządzeniem KRI".
2. Audyt KRI musi być przeprowadzony przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
3. Określenie minimalnego zakresu audytowanych obszarów:
   a) świadczenie usług w formie elektronicznej w tym udostępnionej na platformie ePUAP, zgodnie z art. 16 ust. 1a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2024 poz. 307);
   b) zamieszczenie na głównej stronie internetowej podmiotu (i/lub na stronie BIP), odesłania do opisów usług, które zawierają wymagane informacje dotyczące m.in. aktualnej podstawy prawnej świadczonych usług, nazwy usług, miejsca świadczenia usług (złożenia dokumentów), terminu składania i załatwiania spraw oraz nazwy komórek odpowiedzialnych za załatwienie spraw, zgodnie z § 5 ust. 2 pkt 1 i 4 Rozporządzenia KRI;

c) poziom wspierania modelu usługowego w procesie świadczenia usług elektronicznych przez systemy teleinformatyczne podmiotu, zgodnie z §15 ust. 2 Rozporządzenia KRI;
d) poziom współpracy systemów teleinformatycznych z innymi systemami podmiotu publicznego lub systemami informatycznymi innych podmiotów publicznych w tym rejestrami referencyjnymi, zgodnie z §5 ust. 3 pkt 3 Rozporządzenia KRI;
e) sposób komunikacji z innymi systemami w tym wyposażenie w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami telekomunikacyjnymi za pomocą protokołów komunikacyjnych i szyfrujących zapewniających BI, zgodnie z §16 ust. 1 Rozporządzenia KRI;
f) regulacje wewnętrzne opisujące sposób zarządzania dokumentacją, w tym zakres stosowania elektronicznego obiegu dokumentów, zgodnie z §19 ust. 2 pkt 9 Rozporządzenia KRI;
g) sposób kodowania znaków w dokumentach wysyłanych i odbieranych z systemów teleinformatycznych podmiotu, zgodnie z §17 ust. 1 Rozporządzenia KRI;
h) sposób udostępniania zasobów informatycznych z systemów teleinformatycznych, zgodnie z §18 ust. 1 Rozporządzenia KRI;
i) sposób przyjmowania dokumentów elektronicznych przez systemy teleinformatyczne, zgodnie z §18 ust. 2 Rozporządzenia KRI;
j) dokumentacja SZBI, w tym Polityka BI oraz inne dokumenty stanowiące SZBI, Dokumentacja przeglądów SZBI, szacowania ryzyka, audytów, incydentów naruszenia BI, zgodnie z §19 ust. 1 Rozporządzenia KRI;
k) działania związane z aktualizacją regulacji wewnętrznych w zakresie zmieniającego się otoczenia będące konsekwencją wyników szacowania ryzyka, wniosków z przeglądów SZBI, zaleceń poaudytowych, wniosków z analizy incydentów naruszenia BI, zgodnie z §19 ust. 2 pkt 1 Rozporządzenia KRI;
l) stopień zaangażowania kierownictwa podmiotu w proces ustanawiania i funkcjonowania SZBI oraz zarządzania BI (przeglądy SZBI, szacowanie i obsługa ryzyka BI, egzekwowanie działań związanych z BI), zgodnie z §19 ust. 2 Rozporządzenia KRI;
m) regulacje wewnętrzne opisujące sposób zarządzania ryzykiem BI w podmiocie;
n) dokumentacja z przeprowadzania okresowej analizy ryzyka utraty integralności, poufności lub dostępności informacji, w tym rejestr ryzyk, zawierający informacje o zidentyfikowanych ryzykach, ich poziomie, plan postępowania z ryzykiem, zgodnie z §19 ust. 2 pkt 3 Rozporządzenia KRI;
o) działania minimalizujące ryzyko zgodnie z planem postępowania z ryzykiem stosownie do szacowania ryzyka;
p) regulacje wewnętrzne opisujące sposób zarządzania sprzętem informatycznym i oprogramowaniem (w tym licencjami na oprogramowanie) oraz funkcjonowania rejestru zasobów teleinformatycznych;
q) rejestr zasobów teleinformatycznych zawierający informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku, zgodnie z §19 ust. 2 pkt 2 Rozporządzenia KRI;
r) sposób aktualizacji rejestru zasobów teleinformatycznych;
s) regulacje wewnętrzne opisujące zarządzania uprawnieniami użytkowników do pracy w systemach teleinformatycznych, w tym do przetwarzania danych osobowych;

t) adekwatność poziomu uprawnień do pracy w systemach teleinformatycznych do zakresu czynności i posiadanych upoważnień dostępu do informacji, w tym upoważnień do przetwarzania danych osobowych (rejestr wydanych upoważnień), zgodnie z §19 ust. 2 pkt 4 Rozporządzenia KRI;
u) działania w zakresie monitoringu i kontroli dostępu do zasobów teleinformatycznych, w tym przeglądy w celu wykrywania nieuprawnionego dostępu, nadmiernych uprawnień, konfliktu interesów czy nadzorowania samego siebie itp.;
v) sposób i szybkość odbierania uprawnień byłym pracownikom w systemach informatycznych, zgodnie z §19 ust. 2 pkt 5 Rozporządzenia KRI;
w) regulacje wewnętrzne dotyczące przeprowadzania szkoleń użytkowników zaangażowanych w procesie przetwarzania informacji w systemach teleinformatycznych;
x) dokumentacja z przeprowadzonych szkoleń pod kątem zakresu tematycznego, w tym: aktualności informacji o zagrożeniach, skutkach i zabezpieczeniach, wskaźnik liczby osób przeszkolonych w stosunku do wszystkich osób uczestniczących w procesie przetwarzania informacji, a także cykliczności szkoleń, zgodnie z §19 ust. 2 pkt 6 Rozporządzenia KRI;
y) regulacje wewnętrzne określające zasady bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, zgodne z §19 ust. 2 pkt 8 Rozporządzenia KRI;
z) działania w zakresie stosowania zasad bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, w tym stosowania zabezpieczeń i procedur bezpieczeństwa przez użytkowników urządzeń przenośnych i pracy na odległość;
aa) umowy serwisowe oraz umowy dotyczące rozwoju systemów teleinformatycznych w zakresie zapisów gwarantujących odpowiedni poziom BI, zgodne z §19 ust. 2 pkt 1 Rozporządzenia KRI;
bb) regulacje wewnętrzne, w których określono zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji;
cc) sposób zgłaszania i postępowania z incydentami (działania korygujące), rejestr incydentów naruszenia BI, wpływ analizy incydentów na SZBI, ewentualna współpraca z CERT.GOV.PL, zgodnie z §19 ust. 2 pkt 13 Rozporządzenia KRI;
dd) regulacje wewnętrzne, w których określono zasady przeprowadzania audytów wewnętrznych w zakresie BI;
ee) sprawozdania z audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z §19 ust. 2 pkt 14 Rozporządzenia KRI;
ff) działania podjęte w wyniku zaleceń poaudytowych;
gg) określenie zasad tworzenia, przechowywania oraz testowania kopii zapasowych danych i systemów podmiotu, zgodnie §19 ust. 2 pkt 12 lit. b rozporządzenia KRI;
hh) działania związane z wykonywaniem, przechowywaniem i testowaniem kopii zapasowych danych i systemów oraz dokumentacja z tych działań;
ii) regulacje wewnętrzne, w których ustalono zasady postępowania z informacjami zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, oraz urządzeń mobilnych, w tym plan postępowania z ryzykiem, zgodne z §19 ust. 2 pkt 11 Rozporządzenia KRI;
jj) regulacje wewnętrzne dotyczące zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami poprzez ustalenie zabezpieczeń informacji w sposób uniemożliwiający

nieuprawnionemu jej ujawnienie, modyfikacje usunięcie lub zniszczenie, zgodnie z §19 ust. 2 pkt 7 i 9 Rozporządzenia KRI;

kk) działania związane z monitorowaniem dostępu do informacji np. w systemie informatycznym odnotowującym w bazie danych wszystkie działania użytkowników i administratorów dotyczące systemów teleinformatycznych podmiotu publicznego. Działania związane z monitorowaniem ruchu osobowego w podmiocie, zgodnie z § 19 ust. 2 pkt 7 lit. a) Rozporządzenia KRI;

ll) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji poprzez kontrolę logów systemów, kontrolę wejść i wyjść do pomieszczeń serwerowni, analizę rejestru zgłoszeń serwisowych, analizę rejestru incydentów naruszenia BI, zgodnie z §19 ust. 2 pkt 7 lit. b) Rozporządzenia KRI;

mm) działania związane z zapewnieniem środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych usług sieciowych i aplikacji poprzez stosowanie systemu kontroli dostępu do pomieszczeń serwerowni, systemu autoryzacji dostępu do systemów operacyjnych, sieci i aplikacji, stosowanie zabezpieczeń kryptograficznych, stosowanie systemów antywirusowych i antyspamowych, stosowanie zapór sieciowych typu firewall zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem, zgodnie z § 19 ust. 2 pkt 7 lit. c) Rozporządzenia KRI;

nn) działania związane z ochroną fizyczną informacji zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych, zgodne z wynikami analizy ryzyka i planem postępowania z ryzykiem;

oo) działania związane z utylizacją sprzętu informatycznego i nośników danych a także związane z przekazywaniem sprzętu informatycznego do naprawy w sposób gwarantujący zachowanie BI;

pp) regulacje wewnętrzne, w których ustalono zasady w celu zapewnienia odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych poprzez opisy stosowania zabezpieczeń, w tym plan postępowania z ryzykiem, zgodnie z §19 ust. 2 pkt 12 oraz ust. 4 Rozporządzenia KRI;

qq) regulacje wewnętrzne zawierające zasady prowadzenia i wykorzystania dzienników systemowych (logów), w których odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych, zgodnie z §20 Rozporządzenia KRI;

rr) sposób prezentacji informacji na stronach internetowych systemów telekomunikacyjnych podmiotu oraz zgodność z wymogami WCAG2.1.

4. Na podstawie przeprowadzonej analizy dokumentacji oraz audytu bezpieczeństwa, Wykonawca jest zobowiązany przedstawić pisemny raport zawierający wszystkie wyniki, wnioski wraz z propozycją zmian w zakresie spełnienia wymagań Rozporządzenia KRI. W raporcie muszą zostać uwzględnione wszystkie wyniki cząstkowe z audytowanych obszarów. Spełnienie poszczególnych wymagań zostanie określone w trzyelementowej skali:

   1) spełnione – oznacza, że wymaganie normy zostało całkowicie wdrożone,

   2) częściowo spełnione – może zaistnieć, czy dany obszar został udokumentowany (opracowano stosowną procedurę lub przygotowano inne zabezpieczenie), ale wybrany mechanizm nie został skutecznie wdrożony (np. zdefiniowano strefy bezpieczeństwa, ale system kontroli dostępu nie funkcjonuje poprawnie); najczęstszym przypadkiem oznaczenia wymagania jako „częściowo spełnionego” jest nieskuteczne wdrożenie procedury (nie przestrzeganie zapisów procedury przez pracowników),

3) niespełnione – wymaganie niespełnione oznacza, że nie zostało ono w ogóle zidentyfikowane przez podmiot (podmiot nie jest świadomy danego zagrożenia) lub nie podjęto żadnych działań, aby wdrożyć odpowiednie mechanizmy zabezpieczające.

2. Równoważność rozwiązań

1. Zamawiający informuje, że tam, gdzie Zamawiający opisał przedmiot zamówienia przez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, dopuszcza się rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany udowodnić, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.
2. Zamawiający informuje, że tam, gdzie w Zapytaniu oraz załącznikach opisał przedmiot zamówienia przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty dostarczane przez konkretnego Wykonawcę, co mogłoby doprowadzić do uprzywilejowania lub wyeliminowania niektórych Wykonawców lub produktów, Zamawiający dopuszcza rozwiązanie równoważne opisywanym pod warunkiem, że będą one o nie gorszych właściwościach i jakości. Zamawiający informuje, iż w takiej sytuacji przedmiotowe zapisy są jedynie przykładowe i stanowią wskazanie dla Wykonawcy jakie cechy powinny posiadać materiały użyte do realizacji przedmiotu zamówienia. Ewentualne użycie nazwy producenta ma wyłącznie charakter przykładowy i ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania.
3. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez usługi spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, uwiarygodniających te rozwiązania.
4. Wykonawca, który posługuje się równoważnymi certyfikatami lub normami musi je załączyć do oferty. Przez certyfikat lub normę równoważną Zamawiający rozumie certyfikat lub normę analogiczną co do zakresu z certyfikatami lub normami wskazanymi z nazwy, który potwierdza spełnianie certyfikacji lub normy charakteryzującej się cechami właściwymi dla certyfikacji lub normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do certyfikacji.
5. Za równoważne do normy PN-EN ISO/IEC 27001:2023 Zamawiający uzna inne normy dotyczące międzynarodowego standardu w zakresie bezpieczeństwa informacji obejmujące wymagania normy PN-EN ISO/IEC 27001:2023 określone w rozdziałach 4-10 tej normy.