



Numer sprawy: **IU.271.7.2.2024**

Bartoszyce, dnia 08.10.2024 r.

# Szczegółowy Opis Przedmiotu Zamówienia

## pn. Przeprowadzenie audytu KRI oraz aktualizacja i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji dla Urzędu Miasta Bartoszyce i jego jednostek organizacyjnych

## Spis treści

1.	Przedmiot zamówienia .....	3
1.1.	Zestawienie ilościowe.....	3
1.2.	Wymagania ogólne.....	3
1.3.	Zakup usług aktualizacji i wdrożenia SZBI. ....	6
1.4.	Zakup usług przeprowadzenia audytu zgodności KRI. ....	11
1.5.	Zakup oprogramowania do zarządzania bezpieczeństwem informacji i analizy ryzyka. ....	15
1.5.1.	Wymagania ogólne oprogramowania.....	15
1.5.2.	Wymogi licencjonowania oprogramowania. ....	16
1.5.3.	Wymogi gwarancji oprogramowania.....	16
1.5.4.	Opis funkcjonalny oprogramowania.....	17
1.6.	Zakup usług szkolenia kadry kierowniczej z cyberzagrożeń i wdrożenia SZBI. ....	26
1.7.	Zakup usług szkolenia pracowników z cyberbezpieczeństwa. ....	28
2.	Równoważność rozwiązań.....	30

## 1. Przedmiot zamówienia

### 1.1. Zestawienie ilościowe.

L.p.	Nazwa	Ilość
1.	Zakup usług aktualizacji i wdrożenia SZBI	1 szt.
2.	Zakup usług przeprowadzenia audytu zgodności KRI	1 szt.
3.	Zakup oprogramowania do zarządzania bezpieczeństwem informacji i analizy ryzyka	1 szt.
4.	Zakup usług szkolenia kadry kierowniczej z cyberzagrożeń i wdrożenia SZBI	42 osoby
5.	Zakup usług szkolenia pracowników z cyberbezpieczeństwa	70 osób

### 1.2. Wymagania ogólne.

- Zamówienie będzie realizowane na rzecz Urzędu Miasta Bartoszyce oraz jego następujących jednostek organizacyjnych:
  - Miejski Ośrodek Pomocy Społecznej w Bartoszycach.
  - Środowiskowy Dom Samopomocy w Bartoszycach.
  - Bartoszycki Ośrodek Sportu i Rekreacji.
  - Zakład Usług Komunalnych.
  - Zespół Administracyjny Oświaty w Bartoszycach.
  - Szkoła Podstawowa nr 1 im. Romualda Traugutta w Bartoszycach.
  - Szkoła Podstawowa nr 3 im. Tadeusza Kościuszki w Bartoszycach.
  - Szkoła Podstawowa nr 7 im. Józefa Wybickiego w Bartoszycach.
  - Szkoła Podstawowa nr 8 im. Łesi Ukrainki z Ukraińskim Językiem Nauczania w Bartoszycach.
  - Szkoła Muzyczna I Stopnia w Bartoszycach.
  - Zespół Szkolno-Przedszkolny nr 1 w Bartoszycach.
  - Przedszkole Publiczne nr 2 w Bartoszycach.
  - Integracyjne Przedszkole Publiczne nr 4 w Bartoszycach.
  - Przedszkole Publiczne nr 9 w Bartoszycach.
- Wykonawca jest zobowiązany do przeprowadzenia aktualizacji i wdrożenia kompletnego Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwany: SZBI) dla Zamawiającego.
- Wykonawca jest zobowiązany do dostawy wraz zamówieniem oprogramowania do zarządzania bezpieczeństwem informacji i analizy ryzyka.
- Wykonawca jest zobowiązany do przeprowadzenia szkoleń dla kadry kierowniczej z cyberzagrożeń i wdrożenia SZBI.
- Wykonawca jest zobowiązany do przeprowadzenia szkoleń dla pracowników z cyberbezpieczeństwa.
- Wykonawca jest zobowiązany do przeprowadzenia audytu wdrożonego systemu zarządzania bezpieczeństwem informacji w ramach realizacji 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, 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” dla Zamawiającego.

7. Zakres audytu systemu bezpieczeństwa informacji obejmuje zgodność z kryteriami zawartymi w § 19 ust. 2 ww. rozporządzenia KRI oraz zgodność z wymaganiami normy PN-EN ISO/IEC 27001:2023 dla Zamawiającego.
8. Raport z audytu KRI zostanie podpisany przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczony do Zamawiającego w formie elektronicznej.
9. Audyt KRI oraz aktualizacja i wdrożenie SZBI dla Zamawiającego muszą zostać przeprowadzone przez:
  - a. 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;
  - b. 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.
10. 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 uprawnień SZBI.
11. Wykonawca po wykonaniu 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).
12. Wypełnienie ankiety dojrzałości cyberbezpieczeństwa polegać będzie wypełnieniu przez Wykonawcę kolumn H, I z arkusza „Ankieta” dla Zamawiającego 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.
13. Jednostki samorządu terytorialnego oraz jego 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.

14. 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 uchylającą 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 uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) w polski system prawny Wykonawca ma obowiązek uwzględnić wszystkie ich wymagania przy świadczeniu usług objętych niniejszym zamówieniem zarówno w trakcie realizacji zamówienia jak i w trakcie okresu gwarancji.
15. Zamawiający dopuszcza prowadzenie prac związanych z: analizą dokumentacji, opracowaniem dokumentacji i polityk, opracowaniem 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 siedzibą Zamawiającego.
16. Zamawiający nie dopuszcza aby poszczególne etapy realizacji usługi aktualizacji i wdrożenia SZBI wskazane w dalszej części dokumentu realizowane były w dniach następujących po sobie, Zamawiający zakłada co najmniej 7 dni roboczych przerw pomiędzy etapami. Wymóg dotyczy urzędu i jego jednostek organizacyjnych biorących udział w projekcie.
17. Zamawiający wymaga aby każdy etap (lub jego część) realizacji usługi aktualizacji i wdrożenia SZBI wskazany w dalszej części dokumentu był realizowany w siedzibie Urzędu i jego jednostkach organizacyjnych w czasie nie krótszym niż jeden dzień roboczy odrębnie dla Urzędu i jego jednostek organizacyjnych biorących udział w projekcie.
18. Zamawiający wymaga aby audyt był realizowany w siedzibie Urzędu i jego jednostkach organizacyjnych w czasie nie krótszym niż jeden dzień roboczy odrębnie dla Urzędu i jego jednostek organizacyjnych biorących udział w projekcie.
19. Na wszystkie usługi i dostawy Wykonawca udzieli 24-miesięcznej gwarancji jednak nie dłużej niż do dnia 08.04.2026 r., w tym polegającej na wprowadzaniu niezbędnych zmian w dokumentacji i aktualizacji dokumentacji na podstawie stwierdzonych przez Zamawiającego niezgodności dokumentacji z bieżącym stanem w okresie gwarancji.
20. Zgodnie z wymaganiami Umowy o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0285/FERC.02.02-CS.01-001/23/2024, w przypadku, gdy sposób realizacji zadania będzie wymagał udostępnienia danych osobowych w formie ich powierzenia, Wykonawca będzie zobowiązany do wypełnienia stosownej ankiety bezpieczeństwa systemu ochrony danych

osobowych dostarczonej przez Centrum Projektów Polska Cyfrowa, która stanowi załącznik nr 8 do zapytania ofertowego oraz do zawarcia z Zamawiającym stosownej umowy powierzenia przetwarzania danych osobowych zgodnie ze wzorem stanowiącym załącznik nr 9 do zapytania ofertowego. W przypadku braku akceptacji przez Grantodawcę Projektu „Cyberbezpieczny Samorząd”, tj. Centrum Projektów Polska Cyfrowa na dalsze powierzenie przetwarzanie danych osobowych dla Wykonawcy oferta Wykonawcy zostanie odrzucona.

### 1.3. 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 zgodnie z wymogami ISO/IEC 19011:2002. 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, opracowania 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 wraz z zaleceniami i projektem zmian spełnienie wymagań normy PN-EN ISO/IEC 27001:2023 i zaleceń norm pokrewnych, oraz wymagań prawnych nałożonych na organizację, między innymi 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 zgodnej z wymaganiami normy PN-EN ISO/IEC 27001:2023 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.

Ponad to:

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 dla Zamawiającego.
5. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan postępowania z ryzykiem 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 ryzykiem 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 obsługiwanych 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.

Poszczególne etapy realizacji usługi.

Etap I. Audyt zerowy.

1. Określenie stanu spełnienia wymagań prawnych nałożonych na organizację w zakresie ochrony informacji.
2. Sprawdzenie spełnienia wymagań i zaleceń w ramach KRI i standardów PN-EN ISO/IEC 27001:2023 oraz 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. Analiza stosowanych procedur bezpieczeństwa i zabezpieczeń technicznych w systemach informatycznych na poziomie infrastruktury sieciowej i serwerowej, stacjonarnych i mobilnych stacji roboczych, aplikacji, usług SaaS, serwerów WWW, zewnętrznych nośników danych.
8. Opracowanie raportu z audytu zerowego zawierającego zakres przeprowadzonych prac audytowych, analizę informacji zebranych podczas audytu, wnioski i zalecenia związane z rozwiązaniem występujących problemów, z uwzględnieniem obowiązujących przepisów prawa, zasad wiedzy technicznej, wymagań normy PN-EN ISO/IEC 27001:2023 i zaleceń norm pokrewnych, które zapewnią realizację zobowiązań wskazanych w załączniku nr 6 (Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego i Jednostkach Podległych) do konkursu grantowego.

#### Etap II. 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 wymaganych przez normę PN-EN ISO/IEC 27001:2023;
  - 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 III. 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.

## 1.4. 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 oraz zgodność z wymaganiami normy PN-EN ISO/IEC 27001:2023 dla Zamawiającego 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 normy PN-EN ISO/IEC 27001:2023 oraz 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 użytkownika, 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, zgodnie 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, zgodnie 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, zgodnie 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 użyciem 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 trzelementowej 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.



## 1.5. Zakup oprogramowania do zarządzania bezpieczeństwem informacji i analizy ryzyka.

### 1.5.1. Wymagania ogólne oprogramowania.

1. Dostarczane Oprogramowanie musi w całości posiadać polskojęzyczny interfejs i instrukcję obsługi w języku polskim.
2. Wszystkie komunikaty przekazywane przez system, włącznie z komunikatami o błędach muszą być wyświetlane w języku polskim.
3. Dostarczane Oprogramowanie musi przechowywać wszystkie dane w postaci bazy danych.
4. Dostarczane Oprogramowanie musi umożliwiać pracę na bazie typu Open Source lub na komercyjnym systemie bazodanowym.
5. Dostarczane Oprogramowanie musi cechować się przyjaznym interfejsem użytkownika wykorzystującym: menu, moduły, listy, formularze, przyciski, referencje (linki) itp.
6. Dostarczone Oprogramowanie musi:
  - a. poprawnie działać z minimum 4 najbardziej popularnymi przeglądarkami w Polsce w ich najnowszych wersjach zgodnie ze statystyką prowadzoną na stronie <http://gs.statcounter.com/> za okres 6 miesięcy poprzedzających miesiąc ogłoszenia postępowania określoną dla komputerów stacjonarnych „desktop”,
  - b. umożliwiać pracę jedno i wielostanowiskową oraz zapewniać jednokrotne wprowadzanie danych tak, aby były one widoczne dla wszystkich użytkowników,
  - c. umożliwiać wykorzystanie bezpiecznego protokołu komunikacji pomiędzy stacją roboczą a serwerem, na którym są zainstalowane, w celu zabezpieczenia poufności danych (w zakresie właściwym dla poszczególnych systemów). Wykonawca dostarczy certyfikaty SSL i zapewni ważność co najmniej na okres zaoferowanej gwarancji na Oprogramowanie.
7. Zamawiający wymaga by Oprogramowanie miało jeden, wspólny i spójny interfejs graficzny użytkownika. W szczególności Oprogramowanie musi spełniać minimum następujące wymogi łącznie:
  - a. Jedna, wspólna kolorystyka.
  - b. Spójny wygląd formularzy.
  - c. Podobne operacje muszą być realizowane w ten sam sposób.
  - d. Informacje zwrotne muszą być prezentowane w ten sam sposób.
8. Dostarczone Oprogramowanie musi mieć możliwość uruchomienia na infrastrukturze Zamawiającego lub dostawcy Oprogramowania. Decyzję o miejscu uruchomienia podejmie Zamawiający na etapie realizacji zamówienia, z zastrzeżeniem, że utrzymanie systemu w chmurze SaaS musi odbywać się przy:
  - a. zapewnieniu pełnej funkcjonalności systemu;
  - b. zapewnieniu dostępności systemu w oparciu o umowę SLA na poziomie 99 %;
  - c. zapewnieniu łącza min. 1 Gbps;
  - d. zapewnieniu przestrzeni dla działania systemu bez limitu;
  - e. zapewnieniu certyfikatu SSL;

- f. zapewnieniu kopii zapasowej systemu dla minimum 72 godzin wstecz;
- g. zlokalizowaniu danych na terenie UE.

### 1.5.2. Wymogi licencjonowania oprogramowania.

1. Licencjobiorcą będzie Gmina Miejska Bartoszyce.
2. Licencja powinna umożliwiać działanie oprogramowania do dnia 08.04.2026 r.
3. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
4. Licencja oprogramowania musi umożliwiać działanie systemu w formie usługi chmurowej SaaS.
5. Licencja oprogramowania musi być licencją bez ograniczenia ilości komputerów, na których można używać oprogramowanie.
6. Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych, z wyjątkiem konieczności posiadania dostępu do Internetu.
7. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym komputerze klienckim (licencja nie może być przypisana do komputera/urządzenia).

### 1.5.3. Wymogi gwarancji oprogramowania.

Oprogramowanie powinno zostać objęte gwarancją. Świadczenie usługi gwarancji na oprogramowanie w okresie do dnia 08.04.2026 r. rozpocznie swój bieg w dniu następnym po podpisaniu końcowego protokołu odbioru całego przedmiotu zamówienia przez Zamawiającego. Świadczenie usługi gwarancji ma na celu zapewnienie ciągłości sprawnego działania oprogramowania poprzez realizację działań naprawczych wynikających z analizy ujawnionych problemów, wykrytych błędów i wad Oprogramowania, niewłaściwego działania oprogramowania, spadku wydajności oraz zmian prawnych uniemożliwiających zgodne z prawem funkcjonowanie oprogramowania. W szczególności:

1. Wykonawca zobowiąże się do dostarczania wolnych od wad i zgodnych z aktualnie obowiązującym prawem kolejnych wersji oprogramowania składającego się na przedmiot zamówienia.
2. Wykonawca zobowiąże się do aktualizacji dokumentacji użytkownika i/lub administratora.
3. Wykonawca zapewni w godzinach od 8.00 do 15.30 w dni robocze obecność specjalistów mających niezbędną wiedzę i doświadczenie z zakresu eksploatacji przedmiotu zamówienia, którzy będą odpowiedzialni za przyjmowanie zgłoszeń i realizację działań naprawczych wynikających z analizy ujawnionych problemów, wykrytych błędów i wad Oprogramowania, niewłaściwego działania oprogramowania, spadku wydajności.
4. W ramach gwarancji Wykonawca będzie zobowiązany do nieodpłatnego:
  - a. usuwania błędu, awarii, wady z przyczyn zawinionych przez Wykonawcę będących konsekwencją wystąpienia: błędu w systemie, błędu w dokumentacji administratora lub w dokumentacji użytkownika, błędu w wykonaniu usług przez Wykonawcę;
  - b. usuwania błędu, awarii, wady związanych z realizacją usługi wdrożenia Oprogramowania;

- c. usuwania błędów lub awarii spowodowanych aktualizacjami oprogramowania.
5. Wykonawca będzie musiał informować Zamawiającego o dostępnych aktualizacjach i poprawkach Oprogramowania najpóźniej w ciągu 7 dni od dnia publicznego udostępnienia aktualizacji bądź poprawki o ile za wdrożenie poprawki lub aktualizacji odpowiada Zamawiający.
  6. Zgłaszający, w przypadku wystąpienia błędu, awarii, wady przesyłać będzie do Wykonawcy przy pomocy środków komunikacji formularz zgłoszenia wystąpienia błędu/awarii/wady lub e-mail.
  7. Wykonawca zapewni dostosowanie Oprogramowania do obowiązujących przepisów nie później niż w dniu ich wejścia w życie, chyba że, zmiany prawne nie zostały ogłoszone z minimum 30-dniowym terminem poprzedzającym ich wprowadzenie w życie. W przypadku, jeżeli zmiany nie zostały ogłoszone z minimum 30-dniowym terminem poprzedzającym ich wprowadzenie w życie Wykonawca zobligowany jest do ich wprowadzenia w ciągu 30 dni roboczych od dnia wprowadzenia przepisu w życie.
  8. Zgłoszenia będą klasyfikowane na awarie, błędy i wady:
    - a. Awaria - oznacza sytuację, w której nie jest możliwe prawidłowe użytkowanie Oprogramowania z powodu uszkodzenia lub utraty spójności danych, struktur danych.
    - b. Błąd - niezgodne z dokumentacją użytkową lub wymaganiami Zamawiającego, z instrukcjami lub innymi dokumentami wytworzonymi w czasie wdrożenia działanie oprogramowania;
    - c. Wada - zakłócenie działania oprogramowania polegające na nienależytym działaniu jego części, nie ograniczające działania całego oprogramowania, nie mające istotnego wpływu na zastosowanie oprogramowania i nie będące awarią lub błędem.
  9. Wykonawca zobowiązany będzie do usunięcia awarii, błędów i wad co najmniej w następujących terminach (czas przyjęcia zgłoszenia w przypadku jego dokonania poza godzinami roboczymi, o których mowa w lit. c powyżej, rozpoczyna bieg w kolejnym dniu roboczym):
    - a. Awaria w terminie 2 dni roboczych od przyjęcia zgłoszenia przez Wykonawcę,
    - b. Błędy w terminie 6 dni roboczych od przyjęcia zgłoszenia przez Wykonawcę,
    - c. Wady w terminie 25 dni roboczych od przyjęcia zgłoszenia przez Wykonawcę.

#### 1.5.4. Opis funkcjonalny oprogramowania.

System do zarządzania bezpieczeństwem informacji i analizy ryzyka to system przeznaczony do zarządzania procesem ochrony danych realizujący minimum poniżej określone funkcje.

##### **Autoryzacja.**

1. System musi umożliwić dwuskładnikową formę autoryzacji do systemu.
2. System musi umożliwić co najmniej dwie formy uwierzytelnienia dwuskładnikowego (np. email, sms, aplikacja mobilna, min. Google Authenticator).
3. System musi posiadać opcję resetowania hasła.
4. System musi posiadać mechanizm blokowania dostępu do aplikacji po kilkukrotnym podaniu błędnych danych logowania użytkownika.
5. System musi mieć możliwość ustawienia logowania dla całej puli adresów IP lub tylko dla wybranej.

## **Cześć administracyjna.**

1. System musi umożliwiać administratorowi zarządzanie użytkownikami, w tym:
  - a. Dodanie, edytowanie oraz usunięcie użytkownika,
  - b. Podczas dodawania oraz edycji użytkownika, Administrator musi mieć możliwość określenia dostępu użytkowników do organizacji. Brak dostępu blokuje użytkownikowi dostęp do danych organizacji,
  - c. Umożliwiać anonimizację wybranego użytkownika „na żądanie” oraz po zadanym okresie czasu,
  - d. Umożliwiać Administratorowi blokowanie dostępu do Systemu wybranemu użytkownikowi,
2. System musi posiadać rejestr poprawnych logowań użytkowników.
3. System musi posiadać rejestr nieudanych logowań użytkowników.
4. System musi posiadać rejestr wykonanych czynności w Systemie przez zalogowanego użytkownika.
5. Administrator musi mieć możliwość grupowania poszczególnych uprawnień w role, które następnie mogą zostać przypisane użytkownikowi.
6. System musi umożliwiać administratorowi zarządzanie organizacjami obsługiwanymi w systemie, w tym:
  - a. Dodanie, edytowanie oraz usunięcie organizacji lub przeniesienie do archiwum,
  - b. Podczas dodawania nowej organizacji, administrator musi mieć możliwość wyboru z dostępnej listy czynności przetwarzania te czynności, które po dodaniu, zostaną przypisane automatycznie do rejestru czynności,
  - c. Podczas dodawania oraz edycji organizacji, administrator musi mieć możliwość wpisania danych kontaktowych przedstawiciela podmiotu,
  - d. Podczas dodawania oraz edycji administrator musi mieć możliwość wskazania, którzy użytkownicy będą mieli dostęp do danych organizacji. Brak dostępu użytkownika blokuje dostęp do danych organizacji,
7. System musi umożliwiać administratorowi wysyłanie newsletterów do obsługiwanym organizacjom,
8. Administrator Systemu musi mieć możliwość tworzenia szablonów dokumentów, z których następnie tworzone są czynności nadzorcze,
9. System musi umożliwiać zarządzanie szkoleniami ON-LINE, w tym:
  - a. Dodanie, edytowanie oraz usunięcie szkolenia,
  - b. Podczas dodawania szkolenia, administrator musi mieć możliwość wskazania dla jakich organizacji zostanie udostępnione szkolenie,
  - c. Administrator musi mieć możliwość poinformowania organizacji o dodanym szkoleniu,
  - d. Administrator musi mieć możliwość zmiany (dodania / usunięcia) organizacji, dla której zostało udostępnione szkolenie,
  - e. Administrator musi mieć możliwość wskazania okresu dostępu do szkolenia. Po przekroczeniu daty udostępnienia, szkolenie nie jest dostępne dla pracowników organizacji,
  - f. Administrator musi mieć możliwość zmiany daty udostępnienia szkolenia,
  - g. Administrator musi mieć możliwość tworzenia testów sprawdzających wiedzę po przeprowadzonym szkoleniu przez pracownika,

- h. System musi prezentować wyniki testów dla każdego z pracowników wykonujących szkolenie,
  - i. Administrator musi mieć możliwość ustalenia procentowego poziomu, od którego System uzna test za zaliczony,
  - j. System musi prezentować informację, czy pracownik uzyskał wystarczającą ilość punktów w teście wiedzy,
10. System musi umożliwić administratorowi tworzenie szablonów dokumentów, które następnie zostaną wykorzystane w części dostępnej dla użytkowników obsługujących organizację. Szablony tworzone są co najmniej dla:
- a. Upoważnień,
  - b. Oświadczeń,
  - c. Klauzul informacyjnych,
11. System musi umożliwić administratorowi tworzenie dowolnego szablonu rejestru, który następnie zostanie wykorzystany w części dostępnej dla użytkowników obsługujących organizację.

### **Część obsługi organizacji.**

1. System musi umożliwiać prowadzenie rejestru pracowników, na rzecz których realizowane są zadania związane z ochroną danych, w tym również:
- a. Dodanie, edycję oraz usunięcie pracownika,
  - b. Podczas dodawania oraz edycji, System musi umożliwić wprowadzenie jednego jak i wielu stanowisk dla pracownika,
  - c. Podczas dodawania oraz edycji, System musi umożliwić użytkownikowi wprowadzenie informacji w pole chronione. Dostępność do pola chronionego ustalana jest indywidualnie dla każdego użytkownika organizacji. Jeżeli użytkownik nie jest upoważniony do odczytu pola chronionego, System nie prezentuje zapisanych informacji z tego pola,
  - d. Podczas dodawania oraz edycji, System musi umożliwiać wskazanie czynności przetwarzania do których pracownik ma dostęp,
  - e. W chwili dodania pracownika, musi zostać wysłana informacja o tym zdarzeniu do wskazanych użytkowników Systemu,
  - f. Dla wybranego pracownika, System musi umożliwiać zarządzanie uprawnieniami w systemach IT dostępnych w organizacji,
  - g. System musi umożliwiać wygenerowanie oświadczenia dla wybranego pracownika jak i zbiorczo dla wszystkich pracowników na podstawie wcześniej przygotowanego szablonu,
  - h. System musi umożliwić dodanie upoważnienia dla wybranego pracownika,
  - i. System musi umożliwić wygenerowanie upoważnienia dla wybranego pracownika na podstawie wcześniej przygotowanego szablonu,
  - j. System musi umożliwić cofnięcie upoważnienia dla wybranego pracownika,
  - k. System musi umożliwiać anonimizację pracownika,
  - l. System musi umożliwiać wygenerowanie rejestru pracowników danej organizacji,
  - m. System musi umożliwiać logowanie wybranych pracowników,
  - n. System musi umożliwiać przydzielanie zadań wybranym pracownikom.



2. System musi umożliwiać prowadzenie słownika zagrożeń, w tym:
  - a. Dodanie, edycję oraz usunięcie zagrożenia,
  - b. Podczas dodawania określenie podstawowych parametrów zagrożenia takich jak: nazwy, charakteru zagrożenia (Organizacyjne, Techniczne, IT), prawdopodobieństwa wystąpienia, odpowiedzialnego za dane zagrożenie (wybór ze słownika pracowników lub dodanie odpowiedzianego spoza systemu), określenie dostępności, poufności lub integralności,
  - c. Wygenerowanie do zewnętrznego pliku informacji dotyczących zagrożenia,
  - d. Wygenerowanie do zewnętrznego pliku rejestru zagrożeń.
3. System musi umożliwiać prowadzenie słownika zabezpieczeń, w tym:
  - a. Umożliwiać dodanie, edycję, kopiowanie oraz usunięcie zabezpieczenia,
  - b. Podczas dodawania określenie podstawowych parametrów zabezpieczenia: nazwy, typu zabezpieczenia (Organizacyjne, Techniczne, IT), siły zabezpieczenia, odpowiedzialnego za dane zabezpieczenia (wybór ze słownika pracowników lub dodanie odpowiedzianego spoza systemu),
  - c. Wygenerowanie do zewnętrznego pliku informacji dotyczących zabezpieczenia,
  - d. Wygenerowanie do zewnętrznego pliku rejestru zabezpieczeń.
4. System musi umożliwiać prowadzenie słownika systemów informatycznych, w tym:
  - a. Umożliwiać dodanie, edycję oraz usunięcie systemu,
  - b. Podczas dodawania określenie podstawowych parametrów systemu informatycznego takich jak: nazwy, producenta, ilości dostępnych licencji,
  - c. Prezentację pracowników, którzy mają dostęp do systemu informatycznego,
  - d. Wygenerowanie do zewnętrznego pliku rejestru systemów informatycznych.
5. System musi umożliwiać prowadzenia rejestru obszarów przetwarzania, w tym:
  - a. Dodanie, edycja, kopiowanie oraz usunięcie obszaru,
  - b. Podczas dodawania określenie podstawowych parametrów obszaru takich jak: nazwy, wskazanie obszaru w strukturze organizacji, wskazanie czynności przetwarzania, jakie występują w obszarze, wskazanie występujących zagrożeń dla obszaru,
  - c. Dla zagrożenia znajdującego się w obszarze umożliwić przypisanie zabezpieczeń,
  - d. Prezentować pracowników organizacji, którzy są przypisani dla danego obszaru,
  - e. Wygenerowanie do zewnętrznego pliku rejestru obszarów przetwarzania.
6. System musi umożliwiać prowadzenia rejestru zasobów teleinformatycznych, w tym:
  - a. Dodanie, edycja, kopiowanie oraz usunięcie zasobu,
  - b. Podczas dodawania określenie podstawowych parametrów zasobu takich jak: nazwa, wskazanie zasobu w strukturze organizacji, dodanie informacji o urządzeniach teleinformatycznych znajdujących się w zasobie wraz z osobą odpowiedzialną za urządzenie, wskazanie zagrożeń występujących z zasobie,
  - c. Dla zagrożenia znajdującego się w zasobie umożliwić przypisanie zabezpieczeń,
  - d. Wygenerowanie do zewnętrznego pliku rejestru zasobów teleinformatycznych.
7. System musi umożliwiać prowadzenia dowolnego zasobu, w tym:
  - a. Dodanie, edycja, kopiowanie oraz usunięcie zasobu,



- b. Podczas dodawania określenie podstawowych parametrów zasobu: nazwy, wskazanie zasobu w strukturze organizacji, wskazania elementów występujących w zasobie, wskazanie zagrożeń występujących z zasobie,
  - c. Dla zagrożenia znajdującego się w zasobie umożliwić przypisanie zabezpieczeń,
  - d. Wygenerowanie do zewnętrznego pliku rejestru zasobów.
- 8. System musi umożliwiać prowadzenie dowolnych rejestrów na podstawie szablonów przygotowanych przez administratora, w tym:
  - a. Dodanie, edycja oraz usunięcie rejestru,
  - b. Wygenerowanie do zewnętrznego pliku wybranego rejestru.
- 9. System musi umożliwiać prowadzenie kalendarza, w którym użytkownik ma możliwość dodania zadania.
- 10. System musi umożliwiać dodania lokalnego wzoru szablonu dokumentu na podstawie szablonów przygotowanych przez administratora. Wzory tworzone są co najmniej dla:
  - a. Upoważnień,
  - b. Oświadczeń,
  - c. Klauzul informacyjnych,
- 11. System musi umożliwiać prowadzenie rejestru czynności przetwarzania, w tym:
  - a. Dodanie, edytowanie oraz usunięcie czynności przetwarzania,
  - b. Podczas dodawania określenie podstawowych parametrów czynności takich jak: nazwa, osobę odpowiedzialną za czynność, cel przetwarzania, opis kategorii osób, planowany termin usunięcia kategorii, zakres przetwarzania danych określonych art. 6, zakres przetwarzanych kategorii danych określonych w art. 10, zakres przetwarzanych szczególnych kategorii danych, źródło gromadzenia danych, podstawa prawna przetwarzania zwykłych danych osobowych, podstawa prawna przetwarzania szczególnych kategorii danych osobowych,
  - c. Umożliwić wskazanie systemu, jeżeli czynności dotyczy przetwarzania w systemach teleinformatycznych,
  - d. Umożliwić przeprowadzenie analizy ryzyka praw i wolności dla wskazanej czynności przetwarzania,
  - e. Wygenerowanie do zewnętrznego pliku analizy praw i wolności dla danej czynności przetwarzania,
  - f. Wygenerowanie do zewnętrznego pliku rejestru czynności przetwarzania.
- 12. System musi umożliwiać prowadzenie rejestru kategorii przetwarzania, w tym:
  - a. Dodanie, edytowanie oraz usunięcie rejestru,
  - b. Podczas dodawania określenie podstawowych parametrów rejestru takich jak: nazwa, czy rejestr dotyczy państw trzecich, jeżeli tak wskazanie tych państw, czynności przetwarzania, których rejestr dotyczy, kategorii przetwarzania, zastosowane środki bezpieczeństwa,
  - c. Jeżeli rejestr kategorii został wskazany podczas wprowadzania umowy powierzenia, możliwość wygenerowania rejestru w oparciu o daty z umowy,
  - d. Wygenerowanie do zewnętrznego pliku rejestru kategorii przetwarzania.
- 13. System musi umożliwiać prowadzenie rejestru arkuszy oceny zadania, w tym:
  - a. Dodanie, edytowanie oraz usunięcie arkusza,

- b. Podczas dodawania określenie podstawowych parametrów arkusza takich jak: nazwa, cel zadania, osoba odpowiedzialna za realizację, osoba odpowiedzialna za wdrożenie zadania, informacje o planowanych operacji przetwarzania i celów przetwarzania, informacje o zaangażowaniu podmiotów trzecich i stosowane kodeksy postępowania, informacje ocenie niezbędności i proporcjonalności planowanych czynności przetwarzania,
  - c. Przeprowadzenie analizy ryzyka naruszenia praw i wolności dla wybranego arkusza oceny zadania,
  - d. Przypisanie zabezpieczeń wdrożonych oraz planowanych dla wybranego arkusza oceny zadania,
  - e. Automatyczną aktualizację rejestru czynności przetwarzania danymi z wybranego arkusza oceny zadania,
  - f. Przekazania arkusza oceny zadania do oceny merytorycznej inspektorowi ochrony danych,
  - g. Wygenerowanie do zewnętrznego pliku arkusza oceny zadania.
14. System musi umożliwiać przeprowadzenie testu równowagi dla czynności przetwarzania, w tym:
- a. Dodanie, edytowanie oraz usunięcie testu,
  - b. Podczas dodawania określenie podstawowych parametrów testu takich jak: nazwa, opis przetwarzania danych osobowych i uzasadnienie konieczności jego podjęcia, ustalenie tymczasowej równowagi, zagrożenia związane z ujawnieniem przetwarzanych danych osobowych osobom nieuprawnionym (naruszenie poufności), zagrożenia związane z nieuprawnioną zmianą treści przetwarzanych danych osobowych (naruszeniem integralności), zagrożenia związane z utratą danych lub utratą dostępu do danych (naruszeniem dostępności), dodatkowe gwarancje na rzecz podmiotów danych,
  - c. Wskazanie, której czynności przetwarzania wybrany test dotyczy (jeżeli czynność przetwarzania istnieje),
  - d. Przechowywać archiwalne testy równowagi w przypadku ich zmiany,
  - e. Wygenerowanie do zewnętrznego pliku testu równowagi,
15. System musi umożliwiać prowadzenie rejestru upoważnień, w tym:
- a. Dodanie, edytowanie oraz cofnięcie upoważnienia,
  - b. Podczas dodawania, użytkownik ma mieć możliwość wyboru pracownika jak i wielu pracowników, dla których System doda nowe upoważnienie,
  - c. Podczas dodawania określenie podstawowych parametrów upoważnienia: imię i nazwisko pracownika, stanowisko, data od oraz data do upoważnienia (z możliwością dodania okresu bezterminowego), określenie przetwarzania szczególnych kategorii danych, określenia przetwarzania dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa,
  - d. Edycję numeru upoważnienia,
  - e. Wygenerowanie do zewnętrznego pliku upoważnienia w oparciu o dostępne wzory szablonów dokumentu upoważnienia,
  - f. Zbiorcze wygenerowanie do zewnętrznego pliku upoważnień,
  - g. Wygenerowanie do zewnętrznego pliku rejestru upoważnień.
16. System musi umożliwiać prowadzenie rejestru klauzul informacyjnych, w tym:

- a. Dodanie, edytowanie oraz cofnięcie klauzuli,
  - b. Podczas dodawania klauzuli użytkownik ma mieć możliwość wybrania czynności przetwarzania, których klauzula dotyczy,
  - c. Wygenerowanie do zewnętrznego pliku klauzuli informacyjnej w oparciu o dostępne wzory szablonów dokumentu klauzuli.
17. System musi umożliwiać prowadzenie analizy ryzyka, w tym:
- a. Dodanie nowej analizy ryzyka w oparciu o obszary przetwarzania,
  - b. Możliwości wyboru, którego obszaru przetwarzania dotyczy przygotowanie analizy ryzyka,
  - c. Prezentacji co najmniej: zagrożenia, które występują w danym obszarze, ryzyka początkowego dla wskazanego zagrożenia, ryzyka końcowego dla wskazanego zagrożenia po zastosowaniu zabezpieczeń, prawdopodobieństwo wystąpienia dla wskazanego zagrożenia,
  - d. Możliwość przypisania zalecanych czynności naprawczych dla wskazanego zagrożenia wraz z osobą odpowiedzialną za realizację,
  - e. Wysłanie informacji do osoby odpowiedzialnej za realizację zadania o zaleceniach,
  - f. Wskazania terminu realizacji zaleceń dla zagrożenia,
  - g. Wygenerowanie do zewnętrznego pliku raportu analizy ryzyka.
18. System musi umożliwiać prowadzenie rejestru umów powierzenia, w tym:
- a. Dodanie, edytowanie oraz usunięcia umowy,
  - b. Podczas dodawania określenie podstawowych parametrów umowy: tytuł, data zawarcia umowy, charakter przetwarzania, data powierzenia od oraz do, cel przetwarzania, kategorii osób, których dane dotyczą, zakres powierzanych danych, informację o podmiocie przetwarzającym,
  - c. Wygenerowanie do zewnętrznego pliku umowy powierzenia w oparciu o dostępne wzory szablonów umów,
  - d. Wygenerowanie do zewnętrznego pliku rejestru umów powierzenia.
19. System musi umożliwiać prowadzenie rejestru naruszeń, w tym:
- a. Dodanie oraz edytowanie naruszenia,
  - b. Powiadomić wskazanych użytkowników Systemu o dodaniu nowego naruszenia,
  - c. Podczas dodawania określenie podstawowych parametrów naruszenia takich jak: tytuł, opis zdarzenia, daty wykrycia oraz daty zakończenia (jeżeli jest znana), miejsca wystąpienia, potencjalnych ilości rekordów, opisu okoliczności wystąpienia, wskazania możliwych konsekwencji, wskazania zastosowanych środków bezpieczeństwa, daty zgłoszenia do organu nadzoru (jeżeli dotyczy), daty zawiadomienia właściciela danych (jeżeli dotyczy),
  - d. Umożliwić przeprowadzenie oceny wagi naruszenia wraz z informacją systemową o konieczności wykonania zgłoszenia do UODO lub nie,
  - e. Użytkownik ma mieć możliwość wskazania organu, do którego nastąpiło zgłoszenie wraz z opisem osoby powiadamiającej,
  - f. Użytkownik ma mieć możliwość dodawania czynności, jakie zostały wykonane w ramach obsługi naruszenia,

- g. Zmiana treści naruszenia musi zostać zapisana w systemie wraz z informacją kto dokonał zmiany oraz kiedy została wykonana,
  - h. Wygenerowanie do zewnętrznego pliku oceny wagi naruszenia,
  - i. Wygenerowanie do zewnętrznego pliku rejestru dokonanych zmian w naruszeniu,
  - j. Wygenerowanie do zewnętrznego pliku raportu rejestru naruszeń.
20. System musi umożliwiać prowadzenie rejestru żądań podmiotów, w tym:
- a. Dodanie oraz edytowanie żądania,
  - b. Podczas dodawania określenie podstawowych parametrów żądania takich jak: datę wpływu, źródło żądania, dane wnioskodawcy, treść wraz z kategorią żądania, sposób załatwienia żądania podmiotu,
  - c. Użytkownik musi mieć możliwość przedłużenia realizacji wniosku żądania,
  - d. Wygenerowanie do zewnętrznego pliku rejestru żądań.
21. System musi umożliwiać prowadzenie rejestru czynności nadzorczych realizowanych na rzecz obsługiwanej organizacji, w tym:
- a. Dodanie oraz edytowanie czynności nadzoru na podstawie szablonów dokumentów utworzonych przez Administratora,
  - b. Podczas dodawania czynności określenie podstawowych parametrów czynności nadzorczych takich jak: temat czynności nadzorczej, datę czynności nadzorczej, możliwość dodania czynności nadzorczej do kalendarza organizacji,
  - c. Użytkownik musi mieć możliwość dodania zaleceń do czynności nadzorczej,
  - d. Użytkownik musi mieć możliwość dodania notatki do czynności nadzorczej,
  - e. Wygenerowanie do zewnętrznego pliku raportu z czynności nadzorczej.
22. System musi oferować szkolenia przygotowane przez administratora i udostępnione organizacjom, w tym:
- a. Prezentować listę udostępnionych szkoleń z informacją o dostępności szkolenia,
  - b. Prezentować szczegółowe informacje na temat każdego szkolenia,
  - c. Prezentować listę pracowników, którzy wykonali szkolenie,
  - d. Po zakończeniu szkolenia oraz wykonaniu testu przez pracownika, System musi prezentować wynik testu oraz informację o pozytywnym (lub nie) wyniku wraz z możliwością wygenerowania certyfikatu udziału w szkoleniu.
23. System musi oferować repozytorium plików, w tym:
- a. Możliwość dodawania oraz usunięcia pliku z repozytorium,
  - b. Możliwość grupowania dodawanych plików w katalogi,
  - c. Dodanie pliku wraz z nadaniem hasła zabezpieczającego plik przez nieautoryzowanym dostępem,
  - d. Prezentować podstawową informację o pliku,
  - e. Prezentować informację o pobraniu pliku oraz przez kogo plik został pobrany,
  - f. Udostępniać plik wybranym pracownikom wraz z możliwością potwierdzenia zapoznania się z treścią pliku przez pracownika,
24. System musi oferować zintegrowany moduł HelpDesk, w tym:
- a. Wewnętrzny moduł obsługi zgłoszeń charakteryzujący się:
    - i. Możliwością uwierzytelnienia użytkownika w module tymi samymi danymi jak do Systemu,

- ii. Możliwością prezentacji listy wykonanych zgłoszeń przez użytkowników,
  - iii. Możliwością edycji wykonanego zgłoszenia z zachowaniem pierwotnej treści,
  - iv. Możliwością przypisania prowadzącego lub prowadzących zgłoszenie,
  - v. Możliwością przyjęcia zgłoszenia do realizacji przez użytkownika,
  - vi. Możliwością przypisania kategorii do zgłoszenia,
  - vii. Możliwością wskazania zgłoszenia jako kontynuacja wcześniej dodanego zgłoszenia do modułu,
  - viii. Możliwością dodania komentarza wewnętrznego (dostępnego tylko dla użytkowników wewnętrznego modułu w części obsługi zgłoszeń oraz komentarza dostępnego dla użytkownika, który wykonał zgłoszenie za pomocą funkcjonalności nie wymagającej uwierzytelnienia w module Helpdesk,
  - ix. Możliwością dodania zewnętrznego pliku do zgłoszenia, który w module musi być przechowywany w postaci szyfrowanej,
  - x. Możliwością zamknięcia dodanego zgłoszenia oraz wysłania powiadomienia o zmianie statusu do osoby, która wykonała zgłoszenie,
  - xi. Możliwością wysyłania informacji w postaci uniemożliwiającej osobom postronnym odczytanie informacji (np. ustanowienie hasła dostępu do plików),
- b. Moduł do rejestracji zgłoszeń charakteryzujący się:
- i. Możliwością dodania zgłoszenia przez osoby zalogowane do modułu jak i użytkowników niezalogowanych,
  - ii. Możliwością uwierzytelnienia do modułu tymi samymi danymi jak do Systemu,
  - iii. Możliwością wyświetlania wszystkich zgłoszeń, jakie użytkownik wykonał wraz ze statusami tych zgłoszeń,
  - iv. Możliwością dodania zgłoszenia zawierającego:
    - temat i treść zgłoszenia,
    - kategorię,
    - kontakt do osoby odpowiedzialnej za zgłoszenie,
    - zewnętrzne pliki, które w module muszą być przechowywane w postaci szyfrowanej
  - v. Mechanizmem umożliwiającym podgląd zgłoszenia (np. statusu, komentarzy zewnętrznych) użytkownikowi, który zarejestrował zgłoszenie nie będąc zalogowanym w module,
  - vi. Mechanizmem umożliwiającym podgląd zgłoszenia (np. statusu, komentarzy zewnętrznych) wraz z możliwością dodawania komentarzy lub kolejnych plików zewnętrznych użytkownikowi zalogowanemu w module.
25. System musi udostępniać zbiorcze informacje (statystyki) o danych każdej z obsługiwanych organizacji.
26. Użytkownik Systemu musi mieć możliwość realizacji zgłoszenia dotyczącego ochrony danych osobowych do Inspektora ochrony danych wybranej organizacji.



## 1.6. Zakup usług szkolenia kadry kierowniczej z cyberzagrożeń i wdrożenia SZBI.

### Wymagania ogólne dla szkoleń:

1. Jednostką czasową szkolenia jest 1 godzina szkoleniowa (1 godzina szkolenia = 45 minut).
2. Szkolenia będą trwały maksymalnie 8 godzin szkoleniowych w ciągu dnia.
3. Szkolenia będą odbywać się w dni robocze w godzinach 7.30 – 15.30.
4. Szkolenia będą prowadzone w języku polskim.
5. Szkolenia będą prowadzone w formie stacjonarnej w siedzibie Urzędu Miasta w Bartoszycach.
6. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu prac, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 14 dni przed rozpoczęciem szkolenia.
7. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę.
8. W przypadku szkoleń trwających do 3 godzin, przewiduje się jedną przerwę trwającą 15 minut. W przypadku szkoleń trwających powyżej 3 godzin, organizowane będą dwie przerwy trwające 15 minut każda. Dodatkowo, w przypadku szkoleń trwających 8 godzin zaplanowana jest przerwa trwająca 30 minut.
9. W ramach organizacji szkoleń Zamawiający zapewni rekrutację osób biorących udział w szkoleniach.
10. W ramach organizacji szkoleń Wykonawca zapewni:
  - a. Materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia, harmonogram dzienny szkolenia oraz materiały merytoryczne (np. skrypty, podręczniki, zeszyty informacyjne, broszury) w formie papierowej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Ponadto, uczestnicy otrzymają materiały pisarskie, w tym zeszyty, długopisy, ołówki itp. Materiały szkoleniowe przekazywane są nieodpłatnie Uczestnikom na własność. 2 egzemplarze materiałów szkoleniowych zostaną przekazane Zamawiającemu w celach archiwalnych.
  - b. Projektor multimedialny, tablice i inne artykuły niezbędne do prowadzenia szkoleń.
  - c. Właściwe działania promocyjne i informacyjne dotyczące szkoleń, w tym właściwe oznakowanie sal szkoleniowych, jak również oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych Uczestnikom oraz Zamawiającemu w celach archiwalnych obowiązkowymi oznaczeniami Beneficjentów Funduszy Europejskich.
  - d. Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.
  - e. Kadre trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.
  - f. Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:
    - i. Lista obecności Uczestników szkolenia (dziennie, wypełniane oddzielnie każdego dnia szkolenia).
    - ii. Lista odbioru zaświadczeń o ukończeniu szkolenia.



- iii. Potwierdzenie przez Uczestników odbioru materiałów szkoleniowych.
  - iv. Przeprowadzenie ankiet satysfakcji po każdym szkoleniu.
  - v. Sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.
11. Przy opracowaniu materiałów szkoleniowych Wykonawca zobowiązuje się zapewnić ich zgodność z następującymi zasadami: równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami, równości kobiet i mężczyzn oraz Kartą Praw Podstawowych UE w zakresie dotyczącym zakresu i sposobu realizacji szkoleń. W odniesieniu do wszystkich rozwiązań, m.in. opracowanych dokumentów, szkoleń zapewniony zostanie nieograniczony i równy (bez względu na płeć, rasę, pochodzenie etniczne, religię lub światopogląd, niepełnosprawność, wiek lub orientację seksualną) dostęp dla wszystkich.

#### Ramowy zakres szkolenia:

1. Omówienie zakresu wdrażanego Systemu Zarządzania Bezpieczeństwem Informacji.
2. Przedstawienie zasadniczych zagadnień dokumentacji SZBI.
3. Obowiązki Kierownika Jednostki wynikające z wdrożonego SZBI.
4. Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika.
5. Definicja incydentu bezpieczeństwa i zasady postępowania z incydemem.
6. Rodzaje ataków: ataki socjotechniczne, ataki komputerowe, ataki przez sieci bezprzewodowe, ataki przez pocztę e-mail (fałszywe e-maile), ataki przez strony WWW, ataki przez telefon, phishing, spoofing, spam.
7. Zabezpieczenie informatycznych nośników danych – pamięci i dyski zewnętrzne.
8. Przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych.
9. Prawidłowe korzystanie z oprogramowania antywirusowego.

#### Dodatkowe wymagania:

1. W ramach usługi zostanie przeszkolone 42 osoby w maksymalnie 6 grupach maksimum 8-osobowych.
2. Szkolenie powinno trwać minimum 8 godzin szkoleniowych dla 1 grupy szkoleniowej.

## 1.7. Zakup usług szkolenia pracowników z cyberbezpieczeństwa.

### Wymagania ogólne dla szkoleń:

1. Jednostką czasową szkolenia jest 1 godzina szkoleniowa (1 godzina szkolenia = 45 minut).
2. Szkolenia będą trwały maksymalnie 8 godzin szkoleniowych w ciągu dnia.
3. Szkolenia będą odbywać się w dni robocze w godzinach 7.30 – 15.30.
4. Szkolenia będą prowadzone w języku polskim.
5. Szkolenia będą prowadzone w formie stacjonarnej w siedzibie Urzędu Miasta w Bartoszycach.
6. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu prac, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 14 dni przed rozpoczęciem szkolenia.
7. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę.
8. W przypadku szkoleń trwających do 3 godzin, przewiduje się jedną przerwę trwającą 15 minut. W przypadku szkoleń trwających powyżej 3 godzin, organizowane będą dwie przerwy trwające 15 minut każda. Dodatkowo, w przypadku szkoleń trwających 8 godzin zaplanowana jest przerwa trwająca 30 minut.
9. W ramach organizacji szkoleń Zamawiający zapewni rekrutację osób biorących udział w szkoleniach.
10. W ramach organizacji szkoleń Wykonawca zapewni:
  - a. Materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia, harmonogram dzienny szkolenia oraz materiały merytoryczne (np. skrypty, podręczniki, zeszyty informacyjne, broszury) w formie papierowej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Ponadto, uczestnicy otrzymają materiały pisarskie, w tym zeszyty, długopisy, ołówki itp. Materiały szkoleniowe przekazywane są nieodpłatnie Uczestnikom na własność. 2 egzemplarze materiałów szkoleniowych zostaną przekazane Zamawiającemu w celach archiwalnych.
  - b. Projektor multimedialny, tablice i inne artykuły niezbędne do prowadzenia szkoleń.
  - c. Właściwe działania promocyjne i informacyjne dotyczące szkoleń, w tym właściwe oznakowanie sal szkoleniowych, jak również oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych Uczestnikom oraz Zamawiającemu w celach archiwalnych obowiązkowymi oznaczeniami Beneficjentów Funduszy Europejskich.
  - d. Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.
  - e. Kadre trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.
  - f. Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:
    - i. Lista obecności Uczestników szkolenia (dziennie, wypełniane oddzielnie każdego dnia szkolenia).
    - ii. Lista odbioru zaświadczeń o ukończeniu szkolenia.

- iii. Potwierdzenie przez Uczestników odbioru materiałów szkoleniowych.
  - iv. Przeprowadzenie ankiet satysfakcji po każdym szkoleniu.
  - v. Sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.
11. Przy opracowaniu materiałów szkoleniowych Wykonawca zobowiązuje się zapewnić ich zgodność z następującymi zasadami: równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami, równości kobiet i mężczyzn oraz Kartą Praw Podstawowych UE w zakresie dotyczącym zakresu i sposobu realizacji szkoleń. W odniesieniu do wszystkich rozwiązań, m.in. opracowanych dokumentów, szkoleń zapewniony zostanie nieograniczony i równy (bez względu na płeć, rasę, pochodzenie etniczne, religię lub światopogląd, niepełnosprawność, wiek lub orientację seksualną) dostęp dla wszystkich.

#### Ramowy zakres szkolenia:

1. Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika.
2. Polityka bezpieczeństwa w organizacji.
3. Definicja incydentu bezpieczeństwa i zasady postępowania z incydemem.
4. Rodzaje ataków: ataki socjotechniczne, ataki komputerowe, ataki przez sieci bezprzewodowe, ataki przez pocztę e-mail (fałszywe e-maile), ataki przez strony WWW, ataki przez telefon, phishing, spoofing, spam.
5. Bezpieczeństwo fizyczne - urządzenia, dokumenty, „czyste biurko”.
6. Zabezpieczenie informatycznych nośników danych – pamięci i dyski zewnętrzne.
7. Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.
8. Przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych.
9. Prawidłowe korzystanie z oprogramowania antywirusowego.
10. Zasady aktualizacji programów i aplikacji.
11. Szyfrowanie dokumentów i poczty elektronicznej.
12. Polityka haseł, zarządzanie dostępem i tożsamością.

#### Dodatkowe wymagania:

1. W ramach usługi zostanie przeszkolone 70 osób w maksymalnie 8 grupach maksimum 10-osobowych.
2. Szkolenie powinno trwać minimum 8 godzin szkoleniowych dla 1 grupy szkoleniowej.

## 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.