Załącznik nr 1
do zapytania ofertowego

Opis przedmiotu zamówienia

zapytania ofertowego na realizację usług zwiększenia bezpieczeństwa informacji w Urzędzie Miejskim w Białym Borze w ramach projektu: „Cyberbezpieczny Samorząd w Gminie Biały Bór”.

Definicje

GAP Analysis (Analiza GAP): analiza GAP to metoda używana do oceny różnic między obecnym stanem organizacji a pożądanymi standardami lub celami, w tym przypadku zgodności z normą ISO 27001. Celem analizy GAP jest identyfikacja obszarów wymagających poprawy i rozwój planu działania, aby osiągnąć te cele.

System Zarządzania Bezpieczeństwem Informacji (SZBI): System Zarządzania Bezpieczeństwem Informacji to zorganizowany zestaw polityk, procedur, technologii i zasobów, ustanowionych w celu ochrony i zarządzania bezpieczeństwem informacji w organizacji.

Zgodność z ISO 27001:2022: oznacza spełnianie wymagań tej międzynarodowej normy, która określa, jak organizacje powinny zarządzać bezpieczeństwem informacji, w tym poprzez odpowiednie zarządzanie ryzykiem, zabezpieczenia oraz ciągłe monitorowanie i doskonalenie SZBI.

Luki: w kontekście audytu GAP, luki odnoszą się do różnic między aktualnymi praktykami a wymaganiami określonymi w normie ISO 27001. Luki te mogą być związane z politykami, procedurami, kontrolami czy technologiami i wskazują na obszary, które wymagają ulepszenia w celu osiągnięcia pełnej zgodności z normą.

Załącznik A normy ISO 27001:2022: załącznik A to część normy ISO 27001, która zawiera listę kontroli bezpieczeństwa informacji. Kontrole te są rekomendacjami dotyczącymi zarządzania bezpieczeństwem informacji, które organizacja może wdrożyć, aby zarządzać ryzykiem i zabezpieczyć informacje.

ISO 31000: to międzynarodowa norma dotycząca zarządzania ryzykiem,

Integracja z SZBI: oznacza włączenie procesów, procedur, kontroli i innych elementów zarządzania ryzykiem bezpośrednio do systemu zarządzania bezpieczeństwem informacji zgodnie z normą ISO 27001.

ICT: (skrót ang. “Information and Communications Technology”) TechnologieInformacyjno-Komunikacyjne

Zadania do realizacji w ramach niniejszego zamówienia:

1. Zakup usług opracowywania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z normą ISO 27001, wdrożenia SZBI zgodnie z normą ISO 27001 wraz z opracowaniem Polityki Bezpieczeństwa Informacji (PBI).
2. Zlecenie audytu otwarcia GAP Analysis przez audytora, który posiada ważny certyfikat uprawniający do przeprowadzania audytu w rozumieniu art. 15ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 poz. 913) wskazany w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. poz. 1999).
3. Zakup zewnętrznych szkoleń specjalistycznych oraz materiałów edukacyjnych dla pracowników w kontekście Wdrożonego Systemu Bezpieczeństwa Informacji zgodnie z normą ISO 27001.

Informacje o Zamawiającym mogące mieć wpływ na przygotowanie oferty:
W Urzędzie Miejski w Białym Borze zatrudnionych jest 32 pracowników, którzy realizują zadania w lokalizacji ul. Słupska 10, 78-425 Biały Bór.

I. Przedmiot zamówienia

1. Zadanie 1. Przeprowadzenie audytu otwarcia GAP Analysis.

1.1 Cele audytu otwarcia GAP Analysis

Celem audytu otwarcia GAP Analysis, jest identyfikacja różnic między aktualnym stanem procedur związanych z zarządzaniem bezpieczeństwem informacji w Urzędzie Miejskim w Białym Borze a wymaganiami określonymi w normie ISO 27001:2022. Ten audyt stanowi pierwszy krok do dalszego wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz spełniania wymogów 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. Na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307).

W trakcie audytu otwarcia GAP Analysis, wykonawca musi przeprowadzić ocenę aktualnego stanu procesów związanych z zarządzaniem bezpieczeństwem informacji w kontekście wymagań normy ISO 27001:2022. Kluczowym celem jest identyfikacja „luk" między bieżącymi praktykami zamawiającego a standardami wymaganymi przez normę.

Realizacja audytu otwarcia GAP Analysis przez wykonawcę ma umożliwić efektywne zaplanowanie działań, które będą prowadzić do wdrożenia SZBI oraz osiągnięcia pełnej zgodności z normą ISO 27001:2022.

1.2. Zakres audytu

Wykonawca jest zobowiązany do przeprowadzenia audytu GAP Analysis, który musi obejmować co najmniej następujące elementy:

- Analiza zgodności istniejącej dokumentacji związanej z bezpieczeństwem informacji zamawiającego z wymaganiami ISO 27001:2022, w tym polityk, procedur oraz instrukcji dotyczących bezpieczeństwa informacji.
- Ocena środków technicznych i infrastruktury IT zamawiającego pod kątem ochrony danych i bezpieczeństwa informacji.
- Weryfikacja realizacji i skuteczności wdrożonych kontroli bezpieczeństwa zgodnie z załącznikiem A normy ISO 27001:2022.
- Ocena procesu zarządzania ryzykiem, w tym metod identyfikacji, oceny oraz zarządzania ryzykiem związanym z bezpieczeństwem informacji.
- Ocena roli i zaangażowania kierownictwa oraz kadry kierowniczej zamawiającego w procesy związane z bezpieczeństwem informacji.

W ramach audytu, wykonawca musi zbadać kluczowe obszary i procesy w Urzędzie Miejskim w Białym Borze, które mają bezpośredni wpływ na bezpieczeństwo informacji, w tym:

- Weryfikacja istniejących polityk związanych z bezpieczeństwem informacji zamawiającego, w tym ich aktualności, zrozumiałości i dostępności dla pracowników.
- Analiza sposobów klasyfikacji, etykietowania oraz odpowiedniego obchodzenia się z aktywami informacyjnymi.
- Ocena procedur nadawania, monitorowania i cofania dostępu do informacji i systemów informatycznych.
- Przegląd zabezpieczeń fizycznych miejsc przechowywania informacji, danych i systemów informatycznych.
- Ocena szkoleń, świadomości i zaangażowania pracowników zamawiającego w procesy bezpieczeństwa informacji.
- Analiza procedur identyfikacji, reagowania i zarządzania incydentami bezpieczeństwa.

Jeżeli w trakcie realizacji audytu wykonawca uzna, że konieczne jest zbadanie większej ilości obszarów, procesów lub elementów niż wymienione w opisie, a będzie to niezbędne do osiągnięcia celów audytu, wykonawca jest zobowiązany do przeprowadzenia tych dodatkowych analiz i badań.

1.3. Metodologia oraz harmonogram audytu

W ramach przeprowadzania audytu zamawiający dopuszcza wykorzystywanie różnorodnych technik i narzędzi audytowych, w tym między innymi:

- Bezpośrednie rozmowy z kierownictwem i pracownikami, mające na celu zrozumienie istniejących procedur i praktyk.
- Inspekcje na miejscu w celu oceny fizycznych środków bezpieczeństwa oraz sposób zarządzania i dostępu do systemów informacyjnych.
- Analiza wszystkich istotnych dokumentów związanych z bezpieczeństwem informacji, w tym polityk, procedur operacyjnych oraz zapisów dotyczących incydentów bezpieczeństwa.

Dodatkowo, zamawiający dopuszcza możliwość przeprowadzenia audytu w formie zdalnej, jeżeli okoliczności na to pozwalają. W takim przypadku, wykonawca musi dostarczyć niezbędne narzędzia cyfrowe do komunikacji, gromadzenia i przesyłania danych, aby zapewnić ochronę poufnych informacji i zgodność z najlepszymi praktykami bezpieczeństwa.

Wykonawca jest zobowiązany do dokładnego planowania i harmonogramowania audytu, co zostanie wykonane w ścisłej współpracy z zamawiającym, aby minimalizować zakłócenia w codziennym funkcjonowaniu urzędu. Kluczowe etapy planowania muszą obejmować:

- Zdefiniowanie zakresu audytu, w tym zespołu audytowego oraz szczegółowe ustalenie oczekiwań i celów w porozumieniu z zamawiającym.
- Tworzenie harmonogramu, który precyzyjnie określi czas i daty poszczególnych etapów audytu, w tym wizytacji, wywiadów i przeglądów.
- Realizacja zaplanowanych działań audytowych zgodnie z harmonogramem.
- Opracowanie i przedstawienie szczegółowego raportu z audytu, który zawiera wyniki, zidentyfikowane luki oraz zalecenia, które będą przedstawione zamawiającemu.
- Przygotowanie dodatkowego, skróconego raportu. Skrócony raport powinien obejmować następujące elementy:

1. Streszczenie audytu: Krótki opis zakresu przeprowadzonego audytu oraz metodologii.
2. Kluczowe wnioski: Zwięzłe podsumowanie najważniejszych wniosków audytu, wskazujące na ogólny poziom zgodności z normą ISO 27001 oraz główne obszary wymagające uwagi.
3. Rekomendacje: Ogólne rekomendacje dotyczące działań, które powinny być podjęte w celu poprawy Systemu Zarządzania Bezpieczeństwem Informacji.

Skrócony raport nie powinien zawierać szczegółowych danych technicznych, informacji wrażliwych ani poufnych. Powinien być napisany jasnym i zrozumiałym językiem.

1.4. Procedura przeprowadzenia audytu

Audyt GAP Analysis, przeprowadzany przez wykonawcę w Urzędzie Miejskim w Białym Borze, będzie składał się z kilku kluczowych etapów, które mają na celu kompleksową ocenę i efektywne zidentyfikowanie wszystkich luk w systemie zarządzania bezpieczeństwem informacji. Proces ten musi zostać podzielony co najmniej na następujące etapy:

- **Etap 1** - przygotowanie do audytu. Wykonawca zapozna się wstępnie z organizacją zamawiającego, jej procesami oraz obecnymi procedurami związanymi z bezpieczeństwem informacji. W ramach tego etapu, wykonawca przeprowadzi spotkania z kluczowymi pracownikami oraz kadrą kierowniczą zamawiającego, aby zrozumieć kontekst oraz cel biznesowy organizacji i istniejące struktury oraz praktyki.
- **Etap 2** - rozpoczęcie audytu. Formalne otwarcie audytu odbędzie się podczas spotkania otwierającego z udziałem audytora lub audytorów oraz kierownictwa zamawiającego, w celu przedstawienia planu audytu, omówienia metodologii i potwierdzenia harmonogramu działań.
- **Etap 3** - wykonanie audytu. Na tym etapie, wykonawca musi przeprowadzić szczegółowe badania zgodnie z wcześniej ustalonymi obszarami i procedurami. Działania te mogą obejmować bezpośrednie obserwacje, przegląd dokumentów i systemów oraz przeprowadzenie wywiadów i ankiet z pracownikami zamawiającego.
- **Etap 4** - opracowanie wyników audytu. Wykonawca dokona analizy zebranych danych i sformułuje wnioski dotyczące zgodności z ISO 27001:2022, a także zidentyfikuje luki i przygotuje rekomendacje dla organizacji zamawiającego.
- **Etap 5** - Spotkanie zamykające audyt. Wykonawca przedstawi wstępne wyniki audytu kierownictwu zamawiającego, omówi znalezione luki oraz zaproponowane zalecenia.
- **Etap 6** - Raport końcowy. Wykonawca opracuje szczegółowy i skrócony raport z audytu, który zostanie przedstawiony kierownictwu Urzędu Miejskiego w Białym Borze. Raport ten będzie stanowił podstawę do dalszych działań mających na celu wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji.

Dokumentacja wynikająca z audytu posłuży jako fundament dla dalszych działań mających na celu wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji.

1.5. Struktura zarządzania procesem audytu

Zarządzanie projektem audytu GAP Analysis w Urzędzie Miejskim w Białym Borze musi zostać zorganizowane według klarownej i hierarchicznej struktury, zapewniającej

efektywną komunikację i przepływ informacji między zamawiającym a wykonawcą. Struktura zarządzania projektem musi obejmować:

- **Kierownik projektu (wykonawca).** Osoba odpowiedzialna za nadzór nad całością procesu audytowego, monitorowanie postępów i zarządzanie zasobami. Kierownik projektu będzie również głównym punktem kontaktowym między zespołem audytowym a zamawiającym.
- **Zespół audytowy (wykonawca).** Składający się co najmniej z eksperta ds. audytu oraz jeżeli wykonawca uzna to za niezbędne to również wspierających go audytorów specjalistów. Zespół będzie odpowiedzialny za przeprowadzenie audytu zgodnie z ustalonymi procedurami i standardami.
- **Koordynator ds. bezpieczeństwa (zamawiający).** Osoba odpowiedzialna za koordynację działań po stronie Urzędu, w tym za dostarczanie niezbędnych dokumentów i umożliwienie dostępu do systemów oraz za angażowanie odpowiednich pracowników w proces audytu.

W ramach struktury zarządzania projektem audytu każda z ról będzie miała wyraźnie określone obowiązki:

- **Kierownik Projektu (wykonawca):**

– Zapewnienie zgodności projektu z celami audytu
– Monitorowanie postępów i zarządzanie wszelkimi kwestiami lub ryzykami.
– Raportowanie postępów do kierownictwa Urzędu Miejskiego.
– Zapewnienie zasobów i wsparcia potrzebnego do wykonania audytu.

- **Zespół Audytowy (wykonawca):**

– Przeprowadzenie audytu zgodnie z planem i metodologią.
– Zbieranie danych i przeprowadzanie analiz.
– Opracowywanie raportów audytowych.

- **Koordynator ds. Bezpieczeństwa (zamawiający):**

– Dostarczanie niezbędnych informacji i dokumentów zespołowi audytowemu.
– Organizacja spotkań i dostępu do kluczowych pracowników i zasobów.

1.6 Kryteria akceptacji prac audytowych

Kryteria akceptacji prac audytowych, ustalone przez zamawiającego, obejmują:

- **Zgodność z celami audytu.** Prace wykonane przez wykonawcę muszą w pełni odpowiadać na zdefiniowane przez zamawiającego cele audytu.
- **Dokładność i kompletność.** Raporty audytowe przygotowane przez wykonawcę muszą być kompleksowe, zawierające wszystkie istotne informacje i analizy, które są dokładne i oparte na rzetelnych dowodach.
- **Jasność i zrozumiałość.** Dokumentacja wynikowa, dostarczona przez wykonawcę, musi być jasna, logiczna i łatwa do zrozumienia dla wszystkich

interesariuszy, w tym dla osób niezwiązanych bezpośrednio z procesami IT zamawiającego.

- **Realizacja w ustalonych terminach.** Wykonawca musi zakończyć wszystkie etapy audytu w ramach ustalonych z zamawiającym ram czasowych.

2. Zadanie 2. Opracowywanie pełnej dokumentacji i procedur Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z normą PN-ISO/IEC 27001, w tym Polityki Bezpieczeństwa Informacji oraz wdrożenie ustanowionego SZBI. Zadanie 2. Opracowywanie pełnej dokumentacji i procedur Systemu Zarządzania Bezpieczeństwem

2.1. Zakres zamówienia

Zamówienie obejmuje trzy główne obszary, za które odpowiedzialny będzie wykonawca:

1. **Opracowanie dokumentacji i procedur SZBI.** Wykonawca musi stworzyć kompleksową dokumentację, w tym Polityki Bezpieczeństwa Informacji, procedury operacyjne oraz procedury reagowania na incydenty.
2. **Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji.** Wykonawca musi zaplanować system w strukturach zamawiającego, włączając odpowiednie konfiguracje techniczne i organizacyjne.
3. **Monitorowanie i doskonalenie systemu.** Wykonawca musi zaplanować procesy monitorowania efektywności wdrożonego systemu oraz jego ciągłe doskonalenie.

Opracowanie SZBI ma zapewnić spełnienie wymogów 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. Na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307).

2.2. Opracowanie dokumentacji i procedur SZBI

Struktura i format dokumentacji

Wykonawca musi opracować kompletną dokumentację Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), która będzie zgodna z wymaganiami normy PN-ISO/IEC 27001:2022. Struktura dokumentacji powinna być jasna i zrozumiała dla wszystkich użytkowników systemu w Urzędzie. Dokumentacja ma być zorganizowana w

sposób umożliwiający łatwy dostęp do poszczególnych sekcji i procedur, co ułatwi zarządzanie systemem i jego przegląd. Format dokumentacji powinien obejmować wersje elektroniczne, zapewniające pełną dostępność i możliwość archiwizacji, a także dostępność dla osób o różnych potrzebach, w tym osoby z niepełnosprawnościami oraz promując praktyki zapewniające równość i niedyskryminację. Wersja w postaci papierowej **nie jest wymagana**.

Tworzenie Polityki Bezpieczeństwa Informacji

Wykonawca musi opracować Politykę Bezpieczeństwa Informacji, która stanie się fundamentem dla wszystkich działań związanych z ochroną informacji w Urzędzie. Polityka Bezpieczeństwa Informacji musi określać główne zasady ochrony danych i informacji, cele bezpieczeństwa, a także zobowiązania organizacji do ciągłego doskonalenia SZBI. Polityka Bezpieczeństwa Informacji musi również uwzględniać wymagania prawne, regulacyjne oraz zobowiązania kontraktowe względem klientów i partnerów.

Opracowanie procedur operacyjnych i kontrolnych

Wykonawca musi opracować szczegółowe procedury operacyjne i kontrolne, które umożliwią skuteczne zarządzanie SZBI i odpowiednie reagowanie na incydenty bezpieczeństwa. Procedury te muszą zawierać instrukcje dotyczące zarządzania aktywami, zarządzania dostępem, oceny ryzyka, zarządzania incydentami bezpieczeństwa oraz procedur odzyskiwania danych. Procedury muszą uwzględniać mechanizmy monitorowania i przeglądu efektywności działań bezpieczeństwa, zapewniające ciągłą ochronę informacji zgodnie z najnowszymi standardami i najlepszymi praktykami.

Poniżej przedstawiono przykładową mapę dokumentów, która może posłużyć jako odniesienie dla opracowania dokumentacji SZBI. Wykonawca, po przeprowadzeniu audytu, powinien zaproponować własną mapę dokumentów i procedur, która będzie dostosowana do specyficznych potrzeb Zamawiającego, zapewni zgodność z ISO 27001 oraz umożliwi wykazanie zgodności podczas audytu zgodności z tą normą. Zamawiający dopuszcza modyfikację lub rozbudowę zaproponowanej mapy dokumentów, jeżeli okaże się to konieczne dla skutecznego wdrożenia SZBI.

Mapa dokumentów:

1. Nazwa procedury, polityki, dokumentacji
2. Kontekst organizacji
3. Podręcznik Systemu Zarządzania Bezpieczeństwem Informacji
4. Role, odpowiedzialności i uprawnienia w zakresie bezpieczeństwa informacji

5. Deklaracja wsparcia kierownictwa (wzór)
6. Polityka Bezpieczeństwa Informacji
7. Protokół zebrania (wzór)
8. Cele i plan bezpieczeństwa informacji
9. Proces oceny i zarządzania ryzykiem
10. Raport z oceny ryzyka
11. Plan postępowania z ryzykiem
12. Procedury zmian w SZBI
13. Rejestr zmian SZBI (wzór)
14. Narzędzie do oceny i obróbki ryzyka oparte na aktywach (arkusz kalkulacyjny)
15. Oświadczenie o stosowaniu
16. Narzędzie do oceny i minimalizacji ryzyka na podstawie scenariuszy (arkusz kalkulacyjny)
17. Procedura rozwoju kompetencji w zakresie bezpieczeństwa informacji
18. Procedura komunikacji w zakresie bezpieczeństwa informacji
19. Procedura kontroli dokumentacji
20. Rejestr dokumentacji SZBI
21. Raport z rozwoju kompetencji w zakresie bezpieczeństwa informacji (wzór)
22. Wzajemne powiązania procesów SZBI
23. Proces monitorowania, pomiaru, analizy i oceny
24. Procedura zarządzania niezgodnościami
25. Rejestr niezgodności i działań korekcyjnych (wzór)
26. Harmonogram regularnych działań w SZBI (wzór)
27. Polityka korzystania z mediów społecznościowych
28. Polityka bezpieczeństwa zasobów ludzkich
29. Wytyczne dotyczące segregacji (rozdzielenie) obowiązków wraz z formularzem.
30. Polityka sygnalizacji naruszeń bezpieczeństwa informacji
31. Kontakty z organami władzy
32. Kontakty z grupami zainteresowanych specjalistów
33. Polityka wywiadu w zakresie zagrożeń
34. Proces rozpoznawania zagrożeń
35. Wytyczne bezpieczeństwa informacji dla zarządzania projektami
36. Polityka zarządzania aktywami
37. Inwentaryzacja aktywów informacyjnych
38. Polityka akceptowalnego użytkowania zasobów informacyjnych
39. Polityka dostępu do Internetu
40. Polityka komunikacji elektronicznej
41. Procedura postępowania z aktywami
42. Procedura zarządzania utraconymi lub skradzionymi urządzeniami
43. Polityka współpracy online

44. Lista kontrolna dla nowego pracownika
45. Procedura klasyfikacji informacji ?
46. Procedura etykietowania informacji
47. Procedura przesyłania informacji
48. Polityka kontroli dostępu
49. Proces zarządzania dostępem użytkowników
50. Polityka bezpieczeństwa informacji w relacjach z dostawcami
51. Umowa o bezpieczeństwie informacji z dostawcą (wzór)
52. Procedura oceny należytej staranności dostawcy
53. Ocena należytej staranności dostawcy (arkusz kalkulacyjny)
54. Proces oceny bezpieczeństwa informacji u dostawcy
55. Polityka korzystania z usług chmurowych
56. Proces zarządzania usługami chmurowymi
57. Plan reagowania na incydenty ransomware
58. Plan reagowania na incydenty typu Denial of Service (DoS)
59. Plan reagowania na incydenty naruszenia bezpieczeństwa danych
60. Procedura oceny zdarzeń bezpieczeństwa informacji
61. Procedura reagowania na incydenty bezpieczeństwa informacji
62. Raport z wniosków wyciągniętych z incydentu (wzór)
63. Proces analizy wpływu potencjalnych zdarzeń bezpieczeństwa na organizację
64. Procedura reagowania na incydenty ciągłości działania ICT
65. Plan ciągłości działania ICT
66. Harmonogram ćwiczeń i testów ciągłości działania ICT
67. Plan testów ciągłości działania ICT
68. Raport z testów ciągłości działania ICT (wzór)
69. Procedura wymagań prawnych, regulacyjnych i kontraktowych
70. Wymagania prawne, regulacyjne i kontraktowe
71. Polityka zgodności z prawami własności intelektualnej i prawami autorskimi
72. Procedura weryfikacji pracowników
73. Lista kontrolna weryfikacji pracowników (arkusz kalkulacyjny)
74. Wytyczne dotyczące zapisów do włączenia do umów o pracę
75. Procedura dyscyplinarna dla pracowników
76. Lista kontrolna zakończenia zatrudnienia i zmiany warunków pracy
77. Informacja dla osób odchodzących
78. Wykaz umów o poufności (wzór)
79. Umowa o zachowaniu poufności (wzór)
80. Polityka pracy zdalnej
81. Procedura raportowania zdarzeń bezpieczeństwa informacji
82. Polityka bezpieczeństwa fizycznego
83. Standardy projektowania bezpieczeństwa fizycznego

84. Procedura dostępu do centrum przechowywania danych
85. Polityka monitoringu wizyjnego CCTV
86. Procedura pracy w strefach zabezpieczonych
87. Polityka czystego biurka i czystego ekranu
88. Procedura wynoszenia zasobów poza teren firmy
89. Procedura zarządzania nośnikami wymiennymi
90. Procedura przekazywania nośników fizycznych
91. Harmonogram konserwacji sprzętu (wzór)
92. Procedura utylizacji nośników danych
93. Polityka urządzeń mobilnych
94. Polityka BYOD
95. Polityka dynamicznej kontroli dostępu
96. Polityka przeciwdziałania złośliwemu oprogramowaniu
97. Polityka zarządzania podatnościami technicznymi
98. Procedura oceny podatności technicznych ?
99. Polityka zarządzania konfiguracją
100. Proces zarządzania konfiguracją
101. Polityka usuwania informacji
102. Polityka zapobiegania wyciekom danych
103. Polityka tworzenia kopii zapasowych
104. Polityka zarządzania ciągłością działania
105. Polityka logowania i monitorowania
106. Polityka monitorowania
107. Rejestr programów narzędziowych z uprawnieniami specjalnymi (wzór)
108. Polityka oprogramowania
109. Polityka bezpieczeństwa sieci
110. Obowiązkowe zapisy w umowie o świadczenie usług sieciowych
111. Polityka filtrowania treści internetowych
112. Polityka kryptografii
113. Proces zarządzania zmianami

2.3. Etapy i harmonogram wdrożenia

Etap 1: przygotowanie i zatwierdzenie planu projektowego - wykonawca opracuje i zatwierdzi w porozumieniu z zamawiającym szczegółowy plan wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

Etap 2: zdobycie wsparcia kierownictwa organizacji:

- Wykonawca musi zidentyfikować i omówić specyficzne cele, które kierownictwo zamawiającego chce osiągnąć poprzez wdrożenie systemu, w tym związane z tym korzyści biznesowe i operacyjne. Zadaniem wykonawcy jest zapewnienie, że

cele te są jasno zrozumiałe i że SZBI będzie odpowiednio dostosowany do potrzeb organizacyjnych zamawiającego.

- Wykonawca odpowiedzialny jest za organizację sesji informacyjnych i dyskusji z kluczowymi członkami kierownictwa zamawiającego, aby uzyskać ich opinie, doprecyzować oczekiwania i zbudować silne poparcie dla projektu. Spotkania te będą miały na celu zapewnienie, że wszystkie strony mają jednolite rozumienie zakresu i oczekiwań projektu.

Etap 3: Definicja zakresu SZBI:

- Wykonawca wspólnie z zamawiającym zdefiniuje, które części organizacji, funkcje, dane, lokalizacje i technologie zostaną objęte SZBI. Definicja ta powinna być spójna z celami biznesowymi i operacyjnymi zamawiającego oraz uwzględniać wszystkie zewnętrzne i wewnętrzne wymogi dotyczące bezpieczeństwa informacji.
- Wykonawca przygotuje formalny dokument zakresu SZBI, który zostanie przedłożony do zatwierdzenia przez zamawiającego. Dokument ten będzie zawierał szczegółowy opis zakresu, cele związane z bezpieczeństwem informacji, a także zobowiązania organizacji dotyczące przestrzegania wymogów prawnych i regulacyjnych.
- Wykonawca musi zapewnić, że zakres SZBI jest w pełni zintegrowany z obecnymi procesami biznesowymi oraz infrastrukturą technologiczną zamawiającego, co umożliwi sprawną implementację i późniejsze funkcjonowanie systemu.

Etap 4: Inwentaryzacja zasobów informacyjnych:

- W ramach tego etapu, wykonawca współpracując z zamawiającym, musi przeprowadzić szczegółową inwentaryzację wszystkich zasobów informacyjnych istotnych dla organizacji oraz musi ocenić potencjalne ryzyka związane z ich bezpieczeństwem. Wykonawca musi zidentyfikować i skatalogować wszystkie zasoby informacyjne należące do zamawiającego, które mogą obejmować dane cyfrowe, fizyczne nośniki informacji, oprogramowanie, sprzęt komputerowy oraz infrastrukturę sieciową.
- Po zidentyfikowaniu zasobów, wykonawca wraz z zamawiającym muszą przypisać każdemu z nich poziom ważności i poufności.

Etap 5: Przygotowanie oświadczenia stosowania:

- Wykonawca musi zredagować formalny dokument oświadczenia stosowania.
- Dokument oświadczenia stosowania będzie przedmiotem konsultacji z zamawiającym, aby upewnić się, że wszystkie zainteresowane strony zgadzają

się co do zakresu i charakteru oświadczenia. Następnie dokument zostanie ostatecznie zatwierdzony i przyjęty przez zamawiającego.
- Wykonawca musi zadbać, aby oświadczenie stosowania było zintegrowane z innymi dokumentami i procesami w ramach SZBI, takimi jak polityka bezpieczeństwa, procedury operacyjne oraz plany reagowania na incydenty.

Etap 6: Przygotowanie programu wdrożenia SZBI:

Wykonawca przygotuje plan projektu wdrożenia, który określi kluczowe działania, ich kolejność, przypisane zasoby, odpowiedzialności i terminy. Plan powinien także uwzględniać wszelkie zależności między działaniami oraz sposoby ich zarządzania.

Etap 7: Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI):

- Wykonawca musi wdrożyć wszystkie komponenty SZBI, zapewniając ich integrację oraz funkcjonalność.
- Wykonawca musi opracować i zaimplementować politykę bezpieczeństwa informacji, która będzie integralnie powiązana z kluczowymi procesami biznesowymi zamawiającego. Polityka ta określi standardy, procedury oraz odpowiedzialności związane z zarządzaniem informacjami.
- Wykonawca musi zapewnić, że wszystkie wymagane dokumenty, takie jak polityki, procedury, instrukcje operacyjne i rejestry ryzyka, będą opracowane.
- Wykonawca opracuje szablony dokumentów i narzędzia wspomagające, które będą wykorzystywane w codziennej pracy związanej z SZBI, takie jak formularze do zgłaszania incydentów bezpieczeństwa, checklisty audytowe, narzędzia do monitorowania zgodności itp.
- Wykonawca stworzy i zaimplementuje procedury odpowiedzi na incydenty bezpieczeństwa informacji, które określą, jak identyfikować, reagować i zarządzać incydentami.

Zamawiający wymaga od Wykonawcy opracowania szczegółowego harmonogramu wdrożenia SZBI, który będzie obejmować wszystkie kluczowe etapy projektu, od przygotowania planu projektowego po pełne wdrożenie systemu. Harmonogram ten musi być zatwierdzony przez Zamawiającego przed rozpoczęciem implementacji.

Szczegółowe wymagania dotyczące harmonogramu są następujące:

- Wykonawca musi przygotować szczegółowy harmonogram projektu, który jasno określi sekwencję i czas trwania wdrożenia SZBI, wymienionych poniżej:

- **Etap 1:** Przygotowanie i zatwierdzenie planu projektowego.
- **Etap 2:** Zdobycie wsparcia kierownictwa organizacji.

- **Etap 3:** Definicja zakresu SZBI.
- **Etap 4:** Inwentaryzacja zasobów informacyjnych.
- **Etap 5:** Przygotowanie oświadczenia stosowania.
- **Etap 6:** Przygotowanie programu wdrożenia SZBI.
- **Etap 7:** Wdrożenie SZBI.
    - Harmonogram wdrożenia musi zostać przedłożony zamawiającemu do akceptacji przed rozpoczęciem jakichkolwiek działań w ramach projektu. Zatwierdzenie to musi być udokumentowane i może wymagać modyfikacji na żądanie zamawiającego w celu lepszego dopasowania do warunków operacyjnych zamawiającego.
    - Wykonawca jest zobowiązany do regularnego przeglądu i aktualizacji harmonogramu w odpowiedzi na zmieniające się okoliczności projektu lub na wniosek zamawiającego. Wszelkie zmiany w harmonogramie muszą być niezwłocznie komunikowane zamawiającemu i podlegają jego zatwierdzeniu.
    - Wykonawca jest odpowiedzialny za monitorowanie postępów w realizacji harmonogramu i regularne raportowanie statusu zamawiającemu. Raporty powinny zawierać szczegółowe informacje o ukończonych, bieżących oraz planowanych działaniach, a także o wszelkich wyzwaniach czy odchyleniach od pierwotnego planu.

2.4 Wyznaczanie zespołu projektowego

Wdrożenie ZSBI w Urzędzie Miejskim w Białym Borze musi zostać zorganizowane według klarownej i hierarchicznej struktury, zapewniającej efektywną komunikację i przepływ informacji między zamawiającym a wykonawcą. Struktura zarządzania musi obejmować osoby:

Kierownik projektu wdrożenia SZBI (wykonawca):

Odpowiedzialności:

- Koordynacja wszystkich działań związanych z wdrożeniem SZBI.
- Zapewnienie, że projekt jest zgodny z celami bezpieczeństwa informacyjnego zamawiającego.
- Monitorowanie postępów oraz identyfikacja i zarządzanie ryzykami oraz problemami napotkanymi w trakcie realizacji projektu.
- Regularne raportowanie postępów oraz wszelkich istotnych wydarzeń i osiągnięć do zamawiającego.

Zespół projektowy (wykonawca):

Odpowiedzialności:

- Opracowanie i wdrażanie wszystkich elementów SZBI zgodnie z planem projektowym.
- Zbieranie danych i przeprowadzanie analiz dotyczących bezpieczeństwa informacji w organizacji zamawiającego.
- Opracowywanie dokumentacji wdrożenia, w tym procedur, polityk i planów bezpieczeństwa informacji.
- Współpraca z zamawiającym w celu integracji SZBI z operacjami biznesowymi.

Koordynator ds. bezpieczeństwa (zamawiający):

Odpowiedzialności:

- Dostarczanie niezbędnych informacji i dokumentacji zespołowi projektowemu.
- Organizacja spotkań, warsztatów i sesji szkoleniowych dla zespołu projektowego oraz kluczowych pracowników zamawiającego.
- Zapewnienie dostępu do kluczowych zasobów, takich jak systemy informatyczne, bazy danych oraz pracownicy zamawiającego niezbędni do realizacji projektu.
- Pełnienie roli łącznika między zespołem projektowym a kierownictwem oraz innymi działami w organizacji zamawiającego.

2.5 Zakończenie i formalne przekazanie systemu zarządzania bezpieczeństwem informacji (SZBI)

Wykonawca wraz z zamawiającym muszą przeprowadzić szczegółowy przegląd końcowy SZBI, w tym ocenę zgodności z pierwotnie ustalonymi celami i specyfikacjami. Przegląd ten ma na celu upewnienie się, że wszystkie elementy systemu działają prawidłowo i spełniają wymagania bezpieczeństwa.

Po pomyślnym przeglądzie, projekt wymaga formalnego zatwierdzenia przez zamawiającego. To zatwierdzenie będzie dokumentowane w formie formalnego dokumentu przekazania, który potwierdza pełne przyjęcie projektu.

Wykonawca musi przekazać zamawiającemu kompletną dokumentację systemu, która obejmuje instrukcje obsługi, procedury bezpieczeństwa, polityki oraz wszelkie inne dokumenty niezbędne do zarządzania i utrzymania SZBI.

3. Zadanie 3. Szkolenie specjalistyczne dla pracowników Urzędu Miejskiego w Białym Borze w zakresie wdrożonego SZBI wraz z opracowaniem i udostępnieniem materiałów edukacyjnych.

3.1 Cel szkolenia

Celem szkolenia jest wyposażenie pracowników Urzędu Miejskiego w Białym Borze w niezbędną wiedzę i umiejętności potrzebne do efektywnego wykorzystania i zarządzania Systemem Zarządzania Bezpieczeństwem Informacji (SZBI), zgodnie z normą PN-ISO/IEC 27001. Zamawiający dopuszcza stosowanie normy EN ISO/IEC 27001:2023 [IDT] lub ISO/IEC 27001:2022 [IDT].

Zamawiający oczekuje, że w wyniku szkolenia pracownicy będą mogli nie tylko zrozumieć podstawowe koncepcje i wymogi SZBI, ale także nauczą się praktycznych aspektów związanych z codziennym stosowaniem systemu w pracy urzędniczej.

Wykonawca zobowiązany jest zapewnić, aby szkolenie pokrywało kluczowe obszary takie jak polityki bezpieczeństwa informacji, procedury operacyjne i reagowania na incydenty, zarządzanie ryzykiem, a także prawne i regulacyjne aspekty ochrony danych. Szkolenie powinno również skupić się na umiejętnościach praktycznych, takich jak właściwe postępowanie w przypadku wykrycia zagrożeń dla bezpieczeństwa informacji, oraz na rozwijaniu świadomości i kultury bezpieczeństwa wśród pracowników.

Zamawiający podkreśla znaczenie szkolenia jako integralnej części procesu wdrażania i utrzymywania SZBI, mającej na celu nie tylko zwiększenie kompetencji pracowników, ale także poprawę ogólnego poziomu bezpieczeństwa informacji w Urzędzie. Wykonawca musi więc zaprojektować program szkoleniowy, który jest angażujący, interaktywny i dostosowany do różnych poziomów wiedzy uczestników, aby maksymalizować jego efektywność i zapewnić, że wszystkie cele szkoleniowe są osiągane.

3.2. Przygotowanie materiałów edukacyjnych

Wykonawca musi opracować materiały edukacyjne, które będą służyć jako główne narzędzie do przekazywania wiedzy w trakcie szkolenia. Materiały te muszą być zaprojektowane w sposób umożliwiający łatwe zrozumienie i przyswajanie wiedzy przez uczestników o różnym poziomie zaawansowania oraz różnych potrzebach, w tym osoby z niepełnosprawnościami. Zamawiający wymaga, aby materiały były podzielone na moduły tematyczne, każdy z nich zawierający zarówno teorię, jak i elementy praktyczne, w tym ćwiczenia, studia przypadków i przykładowe scenariusze.

Materiały muszą być dostępne w formatach elektronicznych (np. PDF, prezentacje). Wykonawca musi przygotować zestawy pytań kontrolnych i testów, które pozwolą na ocenę postępów i zrozumienia tematu przez uczestników na każdym etapie szkolenia.

Materiały powinny również zawierać praktyczne wskazówki dotyczące wdrażania polityk i procedur w życie codzienne urzędu, uwzględniając specyfikę i potrzeby Urzędu Miejskiego w Białym Borze oraz promując praktyki zapewniające równość i niedyskryminację.

3.3. Szczegółowy program szkolenia

Wykonawca musi zaprojektować i opracować szczegółowy program szkolenia, który następnie musi zostać przedstawiony zamawiającemu do akceptacji. Program ten musi być dostosowany do potrzeb Urzędu Miejskiego w Białym Borze, zgodnie z wymogami dotyczącymi Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

Kluczowe elementy programu szkolenia

- **Cel szkolenia.** Wykonawca musi jasno zdefiniować cele szkolenia, uwzględniając oczekiwania i wymagania zamawiającego w zakresie podnoszenia kompetencji pracowników w obszarze bezpieczeństwa informacji.
- **Zakres tematyczny.** Wykonawca musi określić zakres tematyczny, który powinien obejmować:

- wprowadzenie do SZBI,
- polityki bezpieczeństwa informacji,
- procedury operacyjne i kontrolne,
- Zarządzanie incydentami bezpieczeństwa.

- **Metodyka nauczania.** Program musi zawierać metody i techniki nauczania, które zostaną użyte do przekazywania wiedzy, np:

- Wykłady teoretyczne,
- Warsztaty praktyczne,
- Symulacje scenariuszy awaryjnych,
- Sesje pytań i odpowiedzi.

- **Harmonogram szkolenia.** Wykonawca opracuje harmonogram szkolenia, który uwzględni czas trwania poszczególnych modułów, przerwy oraz interaktywne sesje. Harmonogram ten powinien być zaplanowany tak, aby maksymalnie wykorzystać czas szkolenia przy jednoczesnym zapewnieniu, że wszystkie tematy zostaną wyczerpująco omówione. Harmonogram musi uwzględniać wszystkie zaplanowane sesje szkoleniowe, w tym daty, godziny oraz przewidywany czas trwania każdego modułu. Wykonawca musi przewidzieć odpowiedni czas na pytania i odpowiedzi oraz na interaktywne dyskusje, aby zwiększyć zaangażowanie uczestników i umożliwić im wyjaśnienie wszelkich wątpliwości.

- **Kryteria oceny i monitorowania postępów uczestników.** Program musi zawierać mechanizmy oceny wiedzy i umiejętności uczestników po zakończeniu szkolenia, co umożliwi wykonawcy i zamawiającemu ocenę skuteczności przeprowadzonego szkolenia (np. indywidualne testy online wypełniane imiennie przez uczestników szkolenia).

Proces akceptacji programu szkolenia

Po opracowaniu programu szkolenia, wykonawca przedstawi go zamawiającemu do akceptacji. Zamawiający przeprowadzi przegląd programu, aby upewnić się, że spełnia on wszystkie wymagane standardy oraz adekwatnie adresuje potrzeby i specyfikę Urzędu Miejskiego w Białym Borze. W razie potrzeby, zamawiający może zaproponować zmiany lub uzupełnienia, które zostaną omówione i wdrożone przez wykonawcę przed ostatecznym zatwierdzeniem programu.

Szkolenie stacjonarne w siedzibie Zamawiającego

Szkolenie musi odbyć się w formie stacjonarnej w siedzibie Zamawiającego. Zamawiający udostępni salę szkoleniową.

Szkolenie musi odbyć się w godzinach i w dniu wcześniej uzgodnionym z Zamawiającym, z uwzględnieniem dostępności uczestników.

Podział na grupy i zróżnicowanie treści

W przypadku szkolenia stacjonarnego w siedzibie zamawiającego, będzie przeprowadzone dla grupy 32 osób.

Dopuszcza się realizację szkolenia z podziałem na dwie grupy jednego dnia roboczego (z zachowaniem 8 godzinowego systemu pracy urzędników). Szkolenia należy przeprowadzać w dni robocze, w godzinach pracy urzędu.