Załącznik nr 1 do SWZ
Opis Przedmiotu Zamówienia

Przeprowadzenie audytu bezpieczeństwa, opracowanie dokumentacji i wdrożenie wraz z pakietem szkoleń Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie Miasta i Gminy Września oraz w Ośrodku Pomocy Społecznej we Wrześni

Spis treści:

1 PODSTAWOWE INFORMACJE DOTYCZĄCE PRZEDMIOTU ZAMÓWIENIA

1.1 Tytuł zamówienia

Przeprowadzenie audytu bezpieczeństwa, opracowanie dokumentacji i wdrożenie wraz z pakietem szkoleń Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie Miasta i Gminy Września oraz w Ośrodku Pomocy Społecznej we Wrześni.

1.2 Wymagania ogólne

1. Zamawiającym jest Gmina Września.

   1.1. Zamówienie stanowi jedno z kluczowych zadań realizowanego przez Gminę Września Grantu pn. „Podniesienie bezpieczeństwa infrastruktury teleinformatycznej i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta i Gminy Września oraz w Ośrodku Pomocy Społecznej we Wrześni" (współfinansowanego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23".

   1.2. Celem prowadzonego Grantu jest „Zintensyfikowanie i usprawnienie procesu wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) wspierającego funkcjonowanie administracji samorządowej Gminy Września (UMiG i OPS) poprzez rozbudowę infrastruktury technicznej, budowanie kompetencji i świadomości z obszaru bezpieczeństwa informacji, w tym w szczególności cyberbezpieczeństwa oraz zapewnienie i wdrożenie rozwiązań organizacyjno-prawnych, a także technicznych gwarantujących w zakresie przetwarzania informacji jej poufność, integralność i dostępność, a także zwiększających odporność infrastruktury technicznej na zagrożenia z zakresu cyberbezpieczeństwa".

2. Miejsce realizacji zamówienia to odpowiednio siedziba:

   2.1. Gminy Września - Urzędu Miasta i Gminy Września (UMiG) ul. Ratuszowa 1, 62-300 Września https://bip.wrzesnia.pl/

   2.2. Ośrodka Pomocy Społecznej (OPS) ul. Fabryczna 14, 62-300 Września https://ops-wrzesnia.biuletyn.net/

3. Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Gminie Września w ramach przedmiotowego zamówienia w obszarze organizacyjnym ww. dwóch jednostek organizacyjnych (UMiG, OPS) musi zostać wykonane w oparciu o wymagania normy PN-EN ISO/IEC 27001:2023-08 oraz ma być zgodne z obowiązującymi w tym zakresie przepisami prawa krajowego i wspólnotowego, w tym szczególności z:

   3.1. Ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2024.1557 t.j.) – skrót UoInf,

   3.2. Rozporządzeniem 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. z 2024 r., poz.773) – skrót KRI,

   3.3. Ustawą z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077 z późn. zm.) – skrót UoKSC,

3.4. Ustawą z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2024 poz. 1513 t.j.),

3.5. Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.) – skrót RODO,

3.6. Dyrektywą 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, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE. L. z 2022 r. Nr 333, str. 80) – skrót NIS2,

4. Zgodność z obowiązującymi przepisami prawa musi być zapewniona wg stanu prawnego na 30 dni przed zakończeniem realizacji zamówienia.

4.1. Powyższe oznacza, iż w przypadku wejścia w życie nowelizacji przepisów prawa dot. UoKSC związanej z wdrożeniem wymagań dyrektywy NIS2 https://legislacja.rcl.gov.pl/projekt/12384504 tj. ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych - przepis ten powinien być uwzględniony w realizacji przedmiotu zamówienia.

5. Zamawiający nie przewiduje certyfikacji SZBI na zgodność z normą PN-EN ISO/IEC 27001:2023-08.

6. Zamawiający zakłada, iż w toku realizacji zamówienia poza oczekiwanym, zasadniczym rezultatem realizacji zamówienia tj. opracowaniem i wdrożeniem SZBI w organizacji UMiG oraz OPS, Wykonawca wypracuje oraz przedstawi Zamawiającemu rekomendacje dot. wspólnych elementów, wzorców dokumentacji SZBI, w tym polityk, procedur bezpieczeństwa informacji w zakresie co najmniej odnoszącym się do wspólnego kontekstu organizacji JST – Gminy Września.

6.1. Wypracowane przez Wykonawcę i rekomendowane dobre praktyki / wzorce zawarte w Raporcie Końcowym z realizacji zamówienia, powinny umożliwić osiągnięcie spójności działań i rezultatów w ramach planowanego przez Zamawiającego wdrożenia (w perspektywie najbliższych lat) kompleksowego SZBI w całej organizacji samorządowej Zamawiającego tj. we wszystkich jednostkach organizacyjnych Gminy Września.

7. Zamawiający oczekuje i wymaga, iż wszelkie działania związane z realizacją niniejszego zamówienia będą prowadzone zgodnie i na podstawie niniejszego opisu przedmiotu zamówienia oraz na podstawie bieżących ustaleń stron (Wykonawcy i Zamawiającego) odpowiednio w podziale informacyjnym, organizacyjnym i decyzyjnym (UMiG i OPS).

7.1. Powyższe oznacza, iż poza elementami wspólnymi realizacji zamówienia, które odnoszą się do istoty opracowania i wdrożenia SZBI, wszelkie prace i uzgodnienia oraz ich wyniki powinny być odpowiednio prowadzone w danej jednostce organizacyjnej, a następnie kierowane do wskazanych w strukturze organizacyjnej Zespołu ds. SZBI osób decyzyjnych upoważnionych przez kierownictwo odpowiednio UMiG oraz OPS.

7.2. Na etapie przygotowania organizacyjnego proponowane podejście organizacyjne powinno zostać omówione celem wypracowania uzgodnionych reguł działania Wykonawcy wspartych przez dostarczone przez niego rozwiązania w zakresie komunikacji zdalnej i prowadzenia repozytorium dokumentacji dla procesu wdrożenia SZBI w UMiG i OPS.

7.2.1. Zależnie od specyfiki oferowanych produktów przez Wykonawcę uwzględniając wspólną infrastrukturę systemową dla UMiG i OPS, Zamawiający zakłada, iż niezbędna odrębność procesu wdrożenia SZBI (organizacyjną i techniczną) dla obu ww. jednostek organizacyjnych uzyska poprzez dostępne w oferowanych produktach Wykonawcy mechanizmy autentykacji i autoryzacji lub – przez odrębną instalację produktów odpowiednio dla UMiG i OPS. Oba rozwiązania są akceptowane przez Zamawiającego.

7.3. Zamawiający dopuszcza możliwość zmiany oczekiwanych rozwiązań organizacyjnych i reguł współdziałania w zakresie sposobu realizacji zamówienia odpowiednio do podjętych wspólnych uzgodnień na etapie prac przygotowawczych, które przełożą się ostatecznie na zakres niezbędnych kompetencji i strukturę organizacyjną Zespołu ds. SZBI oraz ustalone reguły komunikacji i działania stron.

8. Termin wykonania zamówienia nie później niż 6 miesięcy od dnia zawarcia umowy z Wykonawcą z uwzględnieniem kolejności wykonania poszczególnych etapów określonych przez Zamawiającego oraz przez „Harmonogram Realizacji Zamówienia", jaki zostanie opracowany przez Wykonawcę w toku realizacji Etapu 1.

9. Zamówienie zostało podzielone odpowiednio na następujące etapy z uwzględnieniem wstępnie oczekiwanych terminów ich wykonania. I tak:

   9.1. Etap 1. Przygotowanie organizacyjne – w terminie 7 dni od daty zawarcia umowy,

   9.2. Etap 2. Przeprowadzenie audytu „zerowego" – w terminie uzgodnionym z Wykonawcą podczas prac Etapu 1, gdzie punktem odniesienia jest oczekiwany przez Zamawiającego termin 30 dni od daty zakończenia Etapu 1,

   9.3. Etap 3: Pogłębienie analizy organizacji oraz opracowanie dokumentacji SZBI,

   9.4. Etap 4: Zapewnienie wsparcia w procesie wdrożenia SZBI wraz z przeprowadzenie szkoleń,

   9.5. Etap 5: Udzielenie gwarancji jakości oraz opracowanie Raportu Końcowego.

10. Z uwagi na realizację zamówienia w ramach projektu „Cyberbezpieczny Samorząd" Wykonawca jest zobowiązany do:

    10.1. Prowadzenia wspólnej z Zamawiającym polityki informacyjnej, której podstawą dla Zamawiającego są wytyczne w zakresie promocji i polityki informacyjnej, jakie nakłada na Zamawiającego, jako Grantobiorcę Instytucja Pośrednicząca, co dotyczy głównie właściwego oznakowania prowadzonej korespondencji, pism, dokumentów zgodnie z obowiązującymi w tym zakresie wytycznymi.

11. Wykonawca jest zobowiązany w Ofercie uwzględnić całość kosztów realizacji zamówienia, w tym koszty transportu, ubezpieczenia dostawy oferowanych produktów (oprogramowania) oraz inne koszty operacyjne niezbędne dla prawidłowego wykonania zamówienia.

12. Na potrzeby realizacji zamówienia Zamawiający:

    12.1. powoła oddelegowany do współpracy z Wykonawcą Zespół ds. SZBI o strukturze i kompetencjach, jakie wynikać będą bezpośrednio z ustaleń Stron, o których mowa w pkt. 7.3. (z uwagi na specyfikę zamówienia oraz wewnętrzne uwarunkowania po stronie Zamawiającego, tenże utworzy strukturę organizacyjną z uwzględnieniem podziału odpowiedzialności i kompetencji, wyznaczając koordynatorów (tj. Przedstawicieli Zamawiającego w ramach umowy) odpowiednio odrębnie ze strony UMiG oraz OPS),

    12.2. zapewni dostępność pracowników i współpracowników, których udział w realizacji zamówienia z uwagi na specyfikę i przedmiot zamówienia będzie konieczny,

    12.3. zapewni dostęp do informacji, dokumentów / dokumentacji, zasobów i obiektów technicznych oraz infrastruktury teleinformatycznej w zakresie rzeczowym niezbędnym do wykonania zamówienia,

    12.4. zapewni aktywny udział kadry zarządzającej oraz pracowników UMiG i OPS w procesie wdrożenia SZBI, w tym także w przewidzianych szkoleniach z zakresu bezpieczeństwa informacji.

13. Integralną częścią opisu przedmiotu zamówienia są:

    13.1. Załącznik 1: Informacja nt. organizacji i aktywów Zamawiającego

13.2. Załącznik 2: Wymagania dot. rozwiązań wspomagających realizację

13.3. Załącznik 3: Zakres testów bezpieczeństwa

13.4. Załącznik 4: Szkolenia z zakresu bezpieczeństwa informacji

2 SPOSÓB REALIZACJI ZAMÓWIENIA

2.1 Etap 1. Przygotowanie organizacyjne

1. W ramach Etapu 1 na podstawie analizy wstępnej kontekstu organizacji oraz udostępnionych przez Zamawiającego informacji, Wykonawca jest zobowiązany:

   1.1. Opracować „Harmonogram Realizacji Zamówienia" stanowiący uszczegółowienie sposobu wykonania zamówienia,

   1.2. Zapewnić i uruchomić oferowane rozwiązania do:

      1.2.1. komunikacji zdalnej oraz prowadzenia repozytorium dokumentacji tzw. bazy projektowej zawierającej wszystkie uzgodnienia, notatki, raporty powiązane z realizacją zamówienia, a także inne dokumenty (uwzględniając w tym zakresie uzgodnione zasady współpracy i powołany ze strony Zamawiającego Zespół ds. SZBI),

      1.2.2. prowadzenia dokumentacji SZBI (instalacja w środowisku infrastruktury teleinformatycznej Zamawiającego)

   1.3. Przeprowadzić niezbędny instruktaż Zespołu ds. SZBI Zamawiającego z zakresu oferowanego rozwiązania do komunikacji zdalnej oraz prowadzenia repozytorium dokumentacji realizowanego zamówienia.

2. „Harmonogram Realizacji Zamówienia" powinien:

   2.1. Definiować wstępne terminy wykonania Etapów 3-5 – wiążący dla Zamawiającego zgodnie z umową jest termin końcowy realizacji zamówienia,

   2.2. Określać zasady komunikacji i współdziałania Stron określonych w odniesieniu do warunków umowy oraz reguł, jakie wynikać będą z możliwości funkcjonalnych dostarczonego przez Wykonawcę rozwiązania do komunikacji zdalnej oraz prowadzenia dokumentacji z wdrożenia SZBI,

   2.3. Zawierać krótki opis struktury organizacyjnej powołanej do realizacji niniejszego zamówienia po stronie Wykonawcy i Zamawiającego (rola, dane kontaktowe: email, telefon) uwzględniający:

      2.3.1. Co najmniej kluczowy skład personelu Wykonawcy wskazany w Ofercie, w tym oddelegowaną na czas realizacji zamówienia osobę odpowiedzialną za bieżące, operacyjne zarządzanie i koordynację prac zespołu Wykonawcy i współdziałanie z Zamawiającym.

      2.3.2. Oddelegowany do współpracy z Wykonawcą ze strony Zamawiającego tzw. Zespół ds. SZBI obejmujący kadrę zarządzającą UMiG i OPS oraz pracowników z obu tych jednostek (w szczególności dotyczyć to będzie Inspektorów Ochrony danych osobowych (IO) oraz Administratorów IT),

   2.4. Wskazać pierwsze oczekiwane terminy udostępnienia informacji, danych, dokumentów oraz innych zasobów, jakie są w gestii władania Zamawiającego i okażą się niezbędne do realizacji zamówienia, co w szczególności dot. infrastruktury technicznej: teleinformatycznej oraz fizycznej (np. dostęp do obiektów na etapie weryfikacji bezpieczeństwa aktywów fizycznych),

   2.5. Określać (wstępnie) planowane, terminy spotkań zarządczych Kierownika Zadania ze strony Wykonawcy oraz Koordynatora Zadania ze strony Zamawiającego (Kierownika Zespołu ds. SZBI po stronie Zamawiającego) – zgodnie z warunkami umowy - Przedstawicieli Stron odpowiedzialnych za bieżącą koordynację oraz zarządzanie pracami Wykonawcy oraz współpracę Zamawiającego z Wykonawcą.

2.6. Zostać opracowany w formie schematu Gantta np. w programie MS Project lub w innej formie np. tabelarycznej tak, aby zapewnić czytelny podział realizacji zamówienia na poszczególne etapy zarządcze enumeratywnie wskazane w niniejszym dokumencie, z opcją wydzielenia zadań / podzadań lub istotnych zdarzeń projektowych np. tzw. punktów kontrolnych, które umożliwią bardziej ścisłe monitorowanie postępu prac w ramach zamówienia.

2.7. Zachować kolejność i terminy wykonania etapów lub zadań, dla których czas trwania lub kolejność określono jednoznacznie w niniejszym dokumencie, w tym przez podanie liczby dni, miesięcy lub daty.

2.8. Uwzględniać niezbędny czas dla Zamawiającego na weryfikację i odbiór dostarczanych przez Wykonawcę produktów (min. 7 dni roboczych), a dla Wykonawcy niezbędny czas na dostosowanie produktów i uwzględnienie uwag Zamawiającego po ich weryfikacji podczas czynności odbioru.

2.9. Uwzględniać inne uwarunkowania wskazane przez Wykonawcę, jako profesjonalistę w wykonywaniu tego rodzaju zamówień, mające istotny wpływ na prawidłową i terminową realizację zamówienia, w tym spełnienie wymagań Zamawiającego z punktu widzenia celu, jaki określono dla przedmiotu zamówienia, czy też zasad etyki zawodowej, jakie obowiązują personel Wykonawcy.

3. Należy podkreślić, iż dobór metod i technik koordynacji prac w zakresie realizacji zamówienia leży w gestii decyzji Wykonawcy, lecz musi być zaakceptowany przez Zamawiającego, który oczekuje w tym zakresie racjonalnego (nie nadmiarowego), ale przede wszystkim optymalnego doboru metod i technik zarządczych w oparciu o doświadczenie Wykonawcy z realizacji podobnych zamówień.

4. Zamawiający zastrzega, iż zgodnie z umową dokumentowanie uzgodnień w formie notatek ze spotkań stanowiących podstawę do określenia zakresu i sposobu realizacji zamówienia dla opracowania i wdrożenia SZBI - jest w gestii zobowiązań Wykonawcy.

4.1. Proces uzgodnienia, akceptacji notatek ze spotkań powinien zostać dostosowany do warunków oraz możliwości funkcjonalnych oferowanego przez Wykonawcę systemu do komunikacji zdalnej oraz prowadzenia dokumentacji projektowej (tutaj wdrożenia SZBI). Celem takiego podejścia jest usprawnienie bieżących uzgodnień, jakie będą zawierane pomiędzy Stronami.

4.2. W trakcie prac analitycznych oraz audytu Zamawiający wyklucza możliwość stosowania ankiet do samodzielnego wypełnienia przez pracowników Zamawiającego. Niezbędne informacje, o ile nie są dostępne i ustrukturyzowane w formie dokumentów Zamawiającego powinny być pozyskane bezpośrednio przez Wykonawcę w trakcie wywiadów oraz potwierdzone stosowną notatką.

5. Zamawiający dopuszcza możliwość prowadzenia spotkań, wywiadów drogą zdalną (z wykorzystaniem dostarczonego przez Wykonawcę systemu do komunikacji zdalnej), w sytuacji, w której w trakcie tych spotkań nie ma potrzeby bezpośredniego dostępu do zasobów/aktywów na miejscu w siedzibie Zamawiającego lub w jakiejkolwiek innej lokalizacji wskazanej przez adres lub przez wskazanie ilościowe (w UMiG i / lub w OPS) – zgodnie z Załącznikiem 1 lub na podstawie bieżących uzyskanych przez Wykonawcę informacji.

5.1. Przeprowadzenie szkoleń dot. zagadnień cyberbezpieczeństwa oraz dokumentacji SZBI musi być prowadzone na miejscu w siedzibie Zamawiającego.

6. Uzgodnienie i odbiór „Harmonogramu Realizacji Zamówienia" musi być uprzedzone stosownym wprowadzeniem dla Zespołu ds. SZBI w problematykę bezpieczeństwa informacji oraz zagadnienia wymagań normy PN-EN ISO/ IEC 27001:2023-08 oraz pozostałych norm i wymagań, jakie wynikają z realizacji zamówienia. Wszystkie te działania muszą mieścić się w terminie przewidzianym na realizację Etapu 1.

2.2 Etap 2. Przeprowadzenie audytu „zerowego”

1. Wykonawca przeprowadzi audyt we wszystkich obszarach funkcjonowania organizacji odpowiednio oraz zgodnie do wymagań przepisów, jakie wskazano w Rozdz. 1.2 pkt. 3, w tym z uwzględnieniem normy PN-EN ISO/IEC 27001:2023-08 (w skrócie ISO 27001).
2. Zamawiający zakłada, iż wymagane powyższe podejście w zakresie przeprowadzenia audytu w odniesieniu do zgodności z normą PN-EN ISO/ IEC 27001:2023-08 - powinno usprawnić proces opracowania dokumentacji SZBI i wdrożenia SZBI m.in. przez wcześniejsze, stopniowe budowanie świadomości zakresu koniecznych zmian i dostosowania organizacji Zamawiającego do wdrożenia SZBI oraz wymagań obowiązujących przepisów prawa, norm i standardów.
3. Celem audytu „zerowego” jest dokonanie oceny, w jakim stopniu Zamawiający wypełnił i realizuje wymagania w zakresie bezpieczeństwa informacji w kontekście zgodności oraz ustanowienia polityki bezpieczeństwa informacji oraz procedur odpowiednio do aktualnie obowiązujących Zamawiającego wymagań KRI oraz UoKSC, w tym pozostałych przepisów prawa zawartych w Rozdziale 1.2 pkt. 3.
    3.1. Wyniki audytu powinny odpowiedzieć na pytanie, czy Zamawiający (UMiG i OPS) działa zgodnie z narzuconymi przez te dokumenty normami prawnymi i organizacyjnymi.
4. Punktem wyjścia do przeprowadzenia audytu musi być szczegółowa analiza kontekstu organizacji Zamawiającego - wewnętrznego i zewnętrznego (UMiG, OPS).
5. Wykonawca przeprowadzi audyt SZBI m.in. w następujących obszarach:
    5.1. bezpieczeństwo osobowe;
    5.2. bezpieczeństwo fizyczne;
    5.3. bezpieczeństwo teleinformatyczne;
    5.4. analiza ryzyka;
    5.5. ciągłość działania;
    5.6. klasyfikacja informacji;
    5.7. zarządzanie incydentami.
6. Przeprowadzenie audytu w ww. obszarach powinno odbyć się m.in. przez:
    6.1. analizę organizacji odpowiednio UMiG i OPS oraz aktualnie obowiązującej dokumentacji z zakresu SZBI w tych jednostkach,
    6.2. zapoznanie się z obowiązującymi przepisami prawa i dostępnymi regulacjami wewnętrznymi mającymi wpływ na bezpieczeństwo informacji,
    6.3. przegląd obowiązków, realizacji zadań oraz odpowiedzialności po stronie kierownictwa i pracowników,
    6.4. przeprowadzenie wywiadów z kluczowymi osobami z Zespołu ds. SZBI Zamawiającego oraz wskazanymi przez nich pracownikami Zamawiającego, piastującymi funkcje istotne z perspektywy bezpieczeństwa informacji,
    6.5. weryfikację zgodności i aktualności dokumentacji, procedur, instrukcji odpowiednio do zgodności z KRI oraz z normą ISO 27001, w tym w szczególności w zakresie procedur postępowania z ryzykiem,
    6.6. weryfikację i ocenę działań korygujących oraz zapobiegawczych,
    6.7. przeprowadzenie weryfikacji zabezpieczeń fizycznych aktywów,

6.8. weryfikację oraz testy zabezpieczeń w obszarze infrastruktury teleinformatycznej dla infrastruktury technicznej oraz eksploatowanych systemów przez przeprowadzenie testów bezpieczeństwa, co w szczególności dot. środowiska aplikacyjnego web (zakres wymaganych działań w zakresie testów bezpieczeństwa określa Załącznik 2).

6.9. (końcową) identyfikację i analizę luk w organizacji pod kątem zapewnienia bezpieczeństwa informacji oraz spełniania wymagań normy ISO 27001, w tym przez weryfikację i ocenę zastosowanych metod i technik w zakresie bezpieczeństwa informacji odpowiednio do Załącznika A normy ISO 27001.

7. Wyniki audytu „zerowego" Wykonawca powinien przedstawić w formie <Raportu z audytu „zerowego" SZBI>, który zawierać powinien, co najmniej:

7.1. wnioski, zalecenia i rekomendacje mające na celu poprawę bezpieczeństwa Zamawiającego, gdzie w tym dokumencie odrębnie (np. w formie załącznika) powinien być wykazany poziom zgodności z KRI oraz UoKSC odpowiednio do wymagań, jakie przywołane zostały w pkt. 1 niniejszego rozdziału.

7.2. propozycje planu realizacji kolejnych etapów realizacji zamówienia,

7.3. wyniki z testów bezpieczeństwa wraz z komentarzem Wykonawcy i rekomendacjami dot. ewentualnej korekty lub zmiany zastosowanych zabezpieczeń informacji lub wskazaniem podatności.

8. Wyniki audytu muszą być przedstawione Kierownictwu Zamawiającego oraz Zespołowi ds. SZBI przez zaprezentowanie wniosków z audytu oraz rekomendacji.

2.3 Etap 3: Pogłębienie analizy organizacji oraz opracowanie dokumentacji SZBI

1. Na podstawie uzyskanych wyników z audytu "zerowego" przeprowadzonego wg normy ISO 27001 oraz pogłębionej analizy organizacji UMiG i OPS z właściwym zrozumieniem potrzeb i oczekiwań Zamawiającego w zakresie dot. formy i treści dokumentacji z punktu widzenia jej odbiorców *(tj. aby nie mnożyć bytów i fikcji oraz tłumaczyć fakty, jak najprościej – ale zapewnić implementację wymagań przepisów prawa oraz obowiązujących w procesie wdrożenia SZBI norm)* - Wykonawca opracuje projekt dokumentacji SZBI.

2. Dokumentacja SZBI musi zostać opracowana w sposób gwarantujący spełnienie wymagań norm rodziny ISO 27000 w szczególności zgodnie z normą PN-EN ISO/IEC 27001:2023-08 oraz wymaganiami, zaleceniami aktualnych norm PN-ISO/IEC 27002, PN-ISO-27005, a także ISO 31000 w zakresie zarządzania ryzykiem oraz PN-EN-ISO-22301-2020 w zakresie planu ciągłości działania.

3. Opracowanie dokumentacji SZBI musi uwzględniać kontekst organizacji Zamawiającego i musi zawierać m.in.:

3.1. Polityki bezpieczeństwa informacji

3.2. Polityki ochrony danych osobowych

3.3. Zasady bezpieczeństwa teleinformatycznego

3.4. Zasady bezpieczeństwa osobowego

3.5. Zasady bezpieczeństwa prawno-organizacyjnego

3.6. Zasady bezpieczeństwa fizycznego

3.7. Inne niezbędne, wymagane dokumenty (instrukcje, regulaminy) odpowiednio do kontekstu wewnętrznego i zewnętrznego organizacji Zamawiającego.

4. Szczegółowa struktura dokumentacji SZBI, w tym podział na dokumenty, musi być dostosowana odpowiednio do adresata danego dokumentu tj. grupy/stanowiska w organizacji oraz odpowiadać na

przypisane im role w strukturze SZBI. Ponadto, dokumentacja musi spełniać wymagania tzw. wiedzy koniecznej tak, aby każda rola i osoba funkcyjna w organizacji Zamawiającego, miała zapewniony dostęp do dokumentacji w zakresie, w jakim jest to dla niej niezbędne dla realizacji zadań w ramach SZBI oraz zadań przypisanych do stanowiska pracy.

5. Zamawiający wymaga, aby dokumentacja SZBI, w tym w szczególności polityki, procedury, w sposób usystematyzowany oraz jednoznaczny opisywała i regulowała kwestie bezpieczeństwa odnosząc to do obszarów funkcjonowania organizacji. Proponowane przez Wykonawcę i uzgodnione z Zamawiającym metody, techniki stosowania zabezpieczeń muszą wynikać bezpośrednio z analizy i rekomendacji zastosowania zabezpieczeń, jakie określa załącznik A do normy ISO/IEC 27001.

   5.1. Wykonawca jest zobowiązany dokonać pełnej analizy propozycji zabezpieczeń załącznik A do normy PN-EN ISO/IEC 27001-2023-08 w formie tzw. „deklaracji stosowania" - i enumeratywnie uzasadnić wybór, zakres zastosowania – lub brak zasadności użycia z uwagi na kontekst organizacyjny i przyjęte założenia dot. zakresu wdrożenia SZBI.

      5.1.1. Wybór zabezpieczeń powinien uwzględniać możliwości organizacyjne, techniczne i budżetowe Zamawiającego zapewniając zastosowanie podczas realizacji zamówienia rozwiązań wyłącznie dostępnych i możliwych do implementacji tak, aby nie powielać fikcji na etapie wdrożenia SZBI przez użycie zabezpieczeń możliwych do zastosowania dopiero w przyszłej perspektywie czasu.

      5.1.2. Wspomagając przyszły proces utrzymania i rozwoju SZBI Wykonawca powinien poza dokonaniem wyboru i uzgodnieniem z Zamawiającym dostępnych zabezpieczeń uzgodnić dla każdej pozycji „deklaracji stosowania" z Załącznika A normy ISO 27001 (mającej swoje uzasadnienia w organizacji Zamawiającego) – rekomendowane, przyszłe zabezpieczenie zwiększające poziom bezpieczeństwa informacji uwzględniając najbliższe potrzeby oraz możliwości organizacyjne, techniczne i budżetowe Zamawiającego. Zaleca się, aby przyszła „deklaracja stosowania" wsparta została wstępnym szacowaniem ryzyka pozwalającym określić priorytety dla przyszłych zabezpieczeń, co pozwoli z kolei na bardziej optymalne z punktu widzenia celu postępowanie z ryzykiem.

6. W zakresie szacowania i postępowania z ryzykiem w bezpieczeństwie informacji Wykonawca jest zobowiązany przedstawić propozycje metodyki analizy ryzyka w ramach SZBI uwzględniając w tym także (w toku dyskusji) rozwiązania aktualnie przyjęte do stosowania u Zamawiającego.

7. Wykonawca jest zobowiązany przeprowadzić przy współudziale pracowników Zamawiającego:

   7.1. inwentaryzację aktywów związanych z przetwarzaniem informacji wraz z ich klasyfikacją,

   7.2. szacowanie analizy ryzyka zgodnie z przyjętą metodyką oraz przy użyciu dostarczonych przez Wykonawcę do tego narzędzi (Załącznik 2 do OPZ).

8. Opracowana przez Wykonawcę dokumentacja musi zostać przez niego wprowadzona do oferowanego Oprogramowania tj. systemu web służącego do prowadzenia dokumentacji SZBI. Zgodnie z ustaleniami z Zamawiającym, Wykonawca dokona niezbędnej konfiguracji systemu web odpowiednio dla pracowników UMiG oraz OPS z uwzględnieniem ich ról w SZBI.

9. Zgodnie z dobrymi praktykami i rekomendacjami dot. wdrożenia SZBI dokumentacja musi zostać zaakceptowana przez poszczególne szczeble kierownictwa organizacji.

   9.1. Przed przystąpieniem do procesu akceptacji dokumentacji SZBI Wykonawca przeprowadzi niezbędne szkolenia wprowadzające w problematykę bezpieczeństwa informacji w zakresie, w jakim będzie to niezbędne dla zrozumienia celu i istoty proponowanych rozwiązań organizacyjnych i technicznych.

10. Etap 3 uznaje się za wykonany (odebrany) po uzyskaniu akceptacji Zamawiającego dla opracowanej przez Wykonawcę dokumentacji SZBI oraz Planu Wdrożenia SZBI w organizacji Zamawiającego.

10.1. Opracowany przez Wykonawcę i zatwierdzony przez Zamawiającego Plan Wdrożenia SZBI w organizacji Zamawiającego (odpowiednio w UMiG i OPS) musi zawierać wskazanie działań, jakie Zamawiający powinien wprowadzić do organizacji celem skutecznego wdrożenia SZBI przy jednoczesnym zapewnieniu wsparcia ze strony Wykonawcy i leżących po jego stronie zobowiązań, takich jak chociażby przeprowadzenie szkoleń dla pracowników Zamawiającego z zagadnień cyberbezpieczeństwa oraz dokumentacji SZBI i jej stosowalności w ramach tzw. pakietu szkoleń.

2.4 Etap 4: Zapewnienie wsparcia we wdrożeniu SZBI wraz z przeprowadzeniem szkoleń

1. Realizację Etapu 4 oraz świadczeń ze strony Wykonawcy inicjuje Zamawiający przez opublikowanie informacji o przyjęciu do stosowania SZBI publikując z dokumentacji SZBI główny dokument Politykę Bezpieczeństwa Informacji (PBI).

2. Odpowiednio do uzgodnień oraz przyjętych terminów Wykonawca przeprowadzi niezbędne dla prawidłowego wdrożenia SZBI szkolenia w ramach tzw. pakietu szkoleń obejmującego zagadnienia z zakresu bezpieczeństwa informacji oraz przyjętej dokumentacji SZBI, co zostało określone w Załączniku 4 do OPZ.

3. Szkolenia muszą być przeprowadzone uwzględniając w tym, poniższe wymagania:

   3.1. Wszystkie szkolenia muszą odbyć we Wrześni, we wskazanej przez Zamawiającego lokalizacji, w terminach uzgodnionych w dni robocze oraz w godzinach pracy danej jednostki organizacyjnej.

   3.2. Do przeprowadzenia szkoleń Zamawiający:

      3.2.1. wskaże lokalizację szkolenia w jednej z jednostek organizacyjnych Gminy Września, zapewniając zarazem możliwość odbycia szkolenia dla grup odpowiednio dobranych do zdefiniowanych ról w SZBI nie większych niż 20 osób,

      3.2.2. udostępni projektor oraz ekran.

   3.3. Przygotowanie ewentualnej pozostałej infrastruktury szkoleniowej jest w gestii Wykonawcy i powinno być dostosowane do rodzaju szkolenia i liczby osób skierowanych na szkolenia, w szczególności dotyczy to (uzgodnionego) programu szkolenia, materiałów szkoleniowych w wersji papierowej oraz elektronicznej, certyfikatów ze szkoleń, a także dokumentacji z przeprowadzonych szkoleń (listy obecności, wyniki „post testów") .

   3.4. Zamawiający zakłada, iż minimalna liczba godzin na dany pakiet szkolenia to minimum 2 pełne godziny szkolenia, przy czym podany czas jest wyłącznie oceną Zamawiającego i nie powinien ograniczać Wykonawcy w możliwości efektywnego przeprowadzenia szkolenia w większej liczbie godzin, jeżeli zakres i liczność zagadnień wymaga takiego zwiększenia liczby godzin.

   3.5. Zamawiający nie dopuszcza możliwości przeprowadzania szkoleń typu e-learning (on-line) w zastępstwie szkoleń tradycyjnych. Zamawiający może zaakceptować przeprowadzenie szkoleń zdalnie (on-line) dla pewnych grup pracowników wyłącznie w przypadku kiedy szkolenie to będzie prowadzone „na żywo" oraz w taki sposób, aby w każdej chwili dana osoba miała możliwość postawienia pytania, zgłoszenia wątpliwości, uzyskując odwrotnie odpowiedź ze strony osoby prowadzącej.

   3.6. Ponadto, celem zwiększenia skuteczności planowanych szkoleń Zamawiający wymaga, aby szkolenia były w znaczącym stopniu interaktywne oraz poparte przykładami, materiałami multimedialnymi, które uatrakcyjnią istotne treści szkolenia zapewniając dzięki temu łatwiejszy przekaz informacyjny oraz budowanie wiedzy po stronie Zamawiającego. W szczególności dotyczy to szkoleń dedykowanych dla Kierownictwa Zamawiającego, Zespołu ds. SZBI oraz kluczowych ról, jakie zostały zdefiniowane w SZBI.

3.7. Zamawiający wymaga, aby każde szkolenie kończyło się tzw. „post testem", który obejmowałby każdego uczestnika szkolenia. Forma i zakres „post testów" musi być uzgodniona z Zamawiającym przed rozpoczęciem cyklu szkoleń.

3.8. Wynik negatywny z „post testów" na poziomie 20% wyklucza akceptację i odbiór przeprowadzonego szkolenia przez Zamawiającego.

4. Poza ww. szkoleniami Wykonawca zapewni dla Zespołu ds. SZBI oraz kluczowych pracowników Zamawiającego zaangażowanych w proces wdrożenia SZBI usługi wsparcia tzw. usługi wdrożeniowe, jak: konsultacje, szkolenia (poza pakietem szkoleń), opracowanie lub aktualizację dokumentów SZBI lub innych dokumentów powiązanych z procesem wdrożenia SZBI, w tym opracowanie materiałów informacyjnych dot. bezpieczeństwa informacji, prezentacji, co obejmuje także materiały multimedialne.

5. Minimalny zakres wsparcia Wykonawcy w ramach tzw. usług wdrożeniowych nie może być mniejszy niż wymagany łączny wymiar godzin, na który składa się 100 roboczogodzin pracy eksperta ds. bezpieczeństwa / audytora powiększony o liczbę dodatkowych godzin usługi, jaką w tym zakresie Wykonawca zadeklarował w Ofercie w ramach podkryterium wyboru najkorzystniejszej oferty pn. „Dodatkowe godziny usługi wdrożeniowej".

5.1. Zakres świadczeń w ramach usług wdrożeniowych podlegających rozliczeniu obejmuje wyłącznie czas pracy zespołu Wykonawcy na miejscu w siedzibie Zamawiającego (UMiG, OPS), czas pracy uzgodnionych konsultacji zdalnych oraz godziny pracy Zespołu Wykonawcy ustalone z Zamawiającym przeznaczone na wykonanie usługi poza siedzibą Zamawiającego np. na opracowanie oczekiwanego dokumentu lub wydanie opinii.

5.2. Zasady rozliczenia usługi wdrożeniowej reguluje umowa.

6. Końcowym działaniem Wykonawcy razem z Zespołem ds. SZBI jest przeprowadzenie oceny efektów wdrożenia SZBI poprzez ocenę osiągnięcia celów wdrożenia oraz ich miar, jakie zostały określone przez Zamawiającego podczas prac przygotowawczych. Dokonanie oceny zostanie przeprowadzone przez wykonanie przeglądu SZBI oraz audytu wewnętrznego dla wybranych obszarów bezpieczeństwa informacji, gdzie czynności audytu wewnętrznego będę prowadzone przez osoby odpowiedzialne za ten zakres działań i kompetencji w SZBI przy aktywnym udziale zespołu Wykonawcy (eksperta ds. bezpieczeństwa / audytu).

6.1. Z uwagi na istotną wagę zagadnień dot. zapewniania dla organizacji ciągłości działania odpowiednio do wymagań normy PN-EN-ISO-22301-2020 w zakresie dot. planu ciągłości działania oraz opracowanych programów ćwiczeń i testowania rozwiązań i strategii w zakresie zapewniania ciągłości działania przegląd SZBI powinien objąć ocenę przeprowadzonych testów system odtwarzania ciągłości działania tj. poszczególnych procedur i rozwiązań poprzez wykonanie scenariuszy symulujących określone incydenty oraz działania w zakresie odtworzenia potwierdzone ustalonymi regułami walidacji zgodności procesu odtworzenia po danym zdarzeniu.

7. Czynności przeglądu SZBI kończy przeprowadzenie ankiety, której celem jest próba oceny „skuteczności" wdrożenia SZBI z punktu widzenia przydatności systemu w funkcjonowaniu organizacji Zamawiającego. Opracowanie ankiety oraz jej przeprowadzenia jest w gestii zobowiązań Wykonawcy. Ankieta powinna objąć w szczególności obszary bezpieczeństwa informacji, jakie były przedmiotem przeglądu oraz powinna pozwolić na wyciągniecie wniosków, co do użyteczności dokumentacji SZBI, opracowanych polityk, procedur oraz zastosowanych zabezpieczeń.

2.5 Etap 5: Udzielenie gwarancji jakości oraz opracowanie Raportu Końcowego

1. W ramach czynności odbioru końcowego Zamawiający dokona weryfikacji oraz potwierdzenia wypełnienia przez Wykonawcę wszystkich zobowiązań, jakie były przedmiotem realizacji zamówienia, dla których odniesieniem będzie opracowany przez Wykonawcę Raport Końcowy zawierający wnioski i rekomendacje Wykonawcy ze zrealizowanego zamówienia.

2. Podczas prowadzenia przez Zamawiającego czynności odbioru końcowego Wykonawca jest zobowiązany do ścisłego współdziałania z Zamawiającym celem skutecznego doprowadzenia do odbioru, przez co należy rozumieć zobowiązanie do udzielania niezbędnych wyjaśnień, uzupełnienia oraz wypełnienia niezrealizowanych zobowiązań, wynikających ze zgłoszonych przez Zamawiającego uwag i zastrzeżeń.

3. Ponadto, w ramach procedury odbioru Wykonawca:

   3.1. udzieli Zamawiającemu gwarancji jakości wykonania zamówienia zgodnie z wymaganiami na okres 2 lat od daty odbioru końcowego, gdzie w ramach tych świadczeń zapewni m.in. usługi wsparcia podczas przeprowadzanego Audytu końcowego SZBI zgodnie z wymaganiami Grantu przez udzielenie wyjaśnień oraz wprowadzenie niezbędnych korekt do dokumentacji SZBI odpowiednio do uzasadnionych, zgłoszonych uwag ze strony audytora lub podmiotu kontrolującego wykonanie zamówienia (dotyczy to takich podmiotów, jak: Instytucja Pośrednicząca odpowiedzialna za realizację projektu „Cyberbezpieczny Samorząd", RIO, NIK lub inny uprawniony do czynności kontroli organ),

   3.2. przedłoży Raport Końcowy, w którym przedstawi:

      3.2.1. wnioski z przeglądu SZBI przeprowadzonego w ramach Etapu 4 zawierające podsumowanie wyników ankiety (Rozdział 2.4 pkt. 7),

      3.2.2. rekomendacje Wykonawcy odnoszące się do najbliższych działań Zamawiającego, jakie w zakresie utrzymania SZBI powinno zaplanować i podjąć Kierownictwo Zamawiającego oraz Zespół ds. SZBI, aby zapewnić skuteczność wdrożonych strategii w zakresie bezpieczeństwa informacji, odnosząc to przede wszystkim do aspektu ich użyteczność.

4. Wszelkie niezbędne korekty, uzupełnienia, jakie mogą wynikać z wezwania Wykonawcy do usunięcia zidentyfikowanych podczas odbioru uchybień, Wykonawca jest zobowiązany skorygować w terminie wskazanym przez Zamawiającego.

3 ZAŁĄCZNIKI

3.1 Załącznik 1: Informacja nt. wybranych aktywów Zamawiającego

3.1.1 Lokalizacje jednostek oraz stan zatrudnienia

3.1.1.1 Urząd Miasta i Gminy Września (UMiG)

Informacje nt. statutu oraz organizacji Urzędu Miasta i Gminy Września (UMiG) dostępne są w Biuletynie Informacji Publicznej (BIP) adres: https://bip.wrzesnia.pl/.

Urząd Miasta i Gminy zajmuje cztery (4) lokalizacje:

1) siedziba główna – ul. Ratuszowa 1,
2) budynki przy: ul. Chopina 8 oraz 9 oraz Fabryczna 14.

Poza powyższym cztery, inne lokalizacje na terenie miasta Września są wykorzystywane do realizacji zadań urzędu.

UMiG zatrudnia 200 pracowników, w tym: kadra zarządzająca: 29 osób (Burmistrz, Z-ca Burmistrza, Sekretarz, Skarbnik, Naczelnicy Wydziałów – 9, Kierownicy i Z-cy kierowników 15 osób), pracownicy merytoryczni – 143 osoby (w tym 10 strażników miejskich), pracownicy techniczni – 28 osób.

Zadania Inspektora Ochrony (IOD) prowadzone są przez pracownika urzędu. Obsługa informatyczna realizowana jest przez Referat Informatyki zatrudniający 5 osób.

UWAGA: Liczba osób zatrudnionych w UMiG w trakcie realizacji zamówienia może ulec nieznacznej zmianie „ in plus / in minus" – do 2%.

3.1.1.2 Ośrodek Pomocy Społecznej we Wrześni (OPS)

Informacje nt. statutu oraz organizacji Ośrodka Pomocy Społecznej we Wrześni (OPS) dostępne są w Biuletynie Informacji Publicznej (BIP) https://ops-wrzesnia.biuletyn.net/.

Ośrodek zajmuje pięć (5) lokalizacji:

1) ul. Fabryczna 14 - główna siedziba OPS,
2) ul. Słowackiego 39 - oddział OPS,
3) ul. Batorego 8 - Klub Senior+ "Wrzosowisko"
4) ul. Chopina 8 (3 biura) - Punkt Wspierania Społeczności Lokalnej,
5) ul. Wrocławska 32B.

Poza powyższym OPS dysponuje pięcioma lokalami, z których trzy (3) są przeznaczone tzw. mieszkania treningowe oraz jeszcze jedną lokalizacją (własność gminy), która przeznaczona jest na potrzeby realizacji zadań OPS.

OPS zatrudnia 128 pracowników, w tym: kadra zarządzająca - 16 osób (Dyrektor, dwóch zastępców dyrektora, kierownicy – 10 osób, zastępca kierownika – 1 osoba, koordynator zespołu – 2 osoby), pracownicy merytoryczni - 110 osób, pracownicy techniczni - 2 osoby.

Podobnie, jak w przypadku UMiG należy zaznaczyć, iż liczba zatrudnionych pracowników w OPS w trakcie realizacji zamówienia może ulec nieznacznej zmianie – „ in plus / in minus" do 2%.

Z punktu widzenia SZBI i określonych w tym systemie ról (wewnętrznym kontekście organizacyjnym), należy wskazać, iż obsługa informatyczna prowadzona jest przez dwie (2) osoby zatrudnione na umowę zlecenie, natomiast zadania Inspektora Ochrony (IOD) realizuje kancelaria prawna.

3.1.2 Gotowość do wdrożenia SZBI oraz infrastruktura IT

Obie jednostki (UMiG, OPS) zgodnie z przyjętą systematyką dotyczącą ścieżki rozwoju w JST, jaka została określona w Poradniku „Cyberbezpieczny Samorząd" (CS) znajdują się obecnie w „Fazie planowania" oraz „Minimalnego spełnienia niektórych wymagań".

Zarządzanie infrastrukturą teleinformatyczną jest w gestii odpowiedzialności każdej z jednostek odrębnie. Należy jednak zaznaczyć, iż z uwagi na udostępnianą przez Gminę Września infrastrukturę teleinformatyczną na rzecz poszczególnych jednostek organizacyjnych gminy, w tym w szczególności na rzecz OPS - Referat Informatyki (RI) UMiG realizuje zadania wsparcia technicznego wykonując nieformalnie część zadań z zakresu, które można byłoby przypisać do organizacji oraz struktur tzw. Centrum Usług Wspólnych. Takie wnioski można powziąć z uwagi na zakres udostępnianych jednostkom organizacyjnym zasobów infrastruktury teleinformatycznej oraz świadczone w związku z tym usługi wsparcia takie jak: dostęp do (wspólnego) punktu dostępu do sieci Internet, zapewnienie zasobów sieci LAN, obsługa serwerów sprzętowych / wirtualnych, zarządzanie dostępem i zasobami z poziomu usług katalogowych.

Łącznie sieć teleinformatyczna Gminy Września obejmuje ok 1300 punktów końcowych, z czego ok 300 to stanowiska komputerowe w UMiG oraz OPS. Urządzenia sieci teleinformatycznej oraz infrastruktury systemowej (dot. UMiG i OPS) znajdują się w sześciu (6) lokalizacjach.

Zgodnie z podziałem zadań pomiędzy UMiG a OPS w obszarze zarządzania infrastrukturą teleinformatyczną, w tych okolicznościach po stronie OPS pozostaje wyłącznie lokalna obsługa informatyczna urządzeń końcowych, takich jak: komputery, drukarki i zainstalowane oprogramowania dziedzinowe, biurowe.

3.2 Załącznik 2: Wymagania dot. rozwiązań wspomagających realizację zamówienia

1. Celem zwiększenia efektywności procesu realizacji zamówienia, Wykonawca jest zobowiązany dostarczyć:
    1.1. oprogramowanie do komunikacji zdalnej oraz do prowadzenia repozytorium dokumentacji w ramach tzw. bazy projektowej, którego dostępność musi być zapewniona przynajmniej na okres realizacji zamówienia,
    1.2. oprogramowanie do prowadzenia, utrzymania dokumentacji SZBI, które musi zostać zainstalowane w infrastrukturze teleinformatycznej Zamawiającego, przy czym instalacja na infrastrukturze Zamawiającego nie może generować dodatkowych kosztów po stronie Zamawiającego
    1.3. rozwiązania wspomagające szacowanie i postępowanie z ryzykiem odpowiednio do uzgodnionych, wdrażanych procedur, gdzie oczekiwanym produktem finalnym mogą być aktywne formularze oprogramowania biurowego (arkusza kalkulacyjnego) dostępne i poprawnie działające w środowisku pakietu Libre Office tj. aktualnie użytkowanym przez Zamawiającego oprogramowaniu biurowym.
2. Dostarczone oprogramowanie do komunikacji zdalnej oraz do prowadzenia repozytorium musi:
    2.1. Zapewnić działanie z aplikację webową dostępną z poziomu przeglądarki internetowej,
    2.2. Umożliwić jednoczesną pracę wielu użytkowników bez nakładania ograniczeń na ich liczbę, przy czym ewentualne ograniczenia mogą dotyczyć wyłącznie ograniczeń infrastruktury w zakresie jej wydajności,
    2.3. Zapewnić mechanizmy zarządzania użytkownikami, w tym nadawania im uprawnień,
    2.4. Wspomagać czynności zarządzania projektem (czytaj realizacją przedmiotowego zamówienia) – minimum w zakresie procedur komunikacji i powiadamiania,

2.5. Zapewniać mechanizmy autoryzacji dostępu, w tym zastosowanie bezpiecznych połączeń np. z zastosowaniem protokołu TLS (rekomendowane jest zastosowanie dwuskładniowej autoryzacji, dla połączeń zewnętrznych),

2.6. Posiadać co najmniej następujące moduły/narzędzia:

2.6.1. narzędzie do wideokonferencji,

2.6.2. serwer/repozytorium plików,

2.6.3. narzędzie do pracy współdzielonej nad dokumentami.

2.7. Narzędzie do wideokonferencji musi umożliwiać:

2.7.1. Tworzenie wideokonferencji i zapraszanie użytkowników zarejestrowanych i/lub niezarejestrowanych (tzw. gości, zapraszanych np. poprzez link do danej wideokonferencji) w systemie,

2.7.2. Udostępnianie treści/widoku ekranu użytkownika dla uczestników zdalnego spotkania,

2.7.3. Prowadzenie rozmowy również w formie czatu dla każdego pokoju (zdefiniowanej grupy użytkowników),

2.7.4. Identyfikację statusu dostępności użytkownika (przynajmniej w zakresie: aktywny, nieaktywny, zajęty),

2.7.5. Mechanizm powiadomień, w tym wywołań użytkowników w trybie czatu.

2.8. Serwer/repozytorium plików powinien umożliwiać:

2.8.1. Tworzenie katalogów projektowych,

2.8.2. Udostępnianie katalogów w ramach zdefiniowanych grup użytkowników lub bezpośrednio użytkownikom w dwóch trybach: tylko podglądu lub pełnego dostępu i edycji dokumentów,

2.9. Narzędzie do pracy współdzielonej nad dokumentami musi zapewnić:

2.9.1. Pracę na dokumentach tekstowych, arkuszach kalkulacyjnych i prezentacjach,

2.9.2. Edycję dokumentu przez wielu użytkowników jednocześnie,

2.9.3. Włączenie trybu śledzenia zmian oraz wykorzystania komentarzy w ramach pracy wspólnej na dokumentach tekstowych,

2.9.4. Identyfikację wersji dokumentów (zapis automatyczny),

2.9.5. Obsługę plików w formacie: docx, xlsx, pptx (lub w formatach open source).

3. Oprogramowania do prowadzenia dokumentacji SZBI musi:

3.1. Być wykonane w technologii WEB oraz dostępne z poziomu przeglądarki,

3.2. Umożliwiać autentykację użytkowników oraz autoryzację dostępu do zasobów SZBI,

3.3. Zapewniać zarządzanie uprawnieniami użytkowników SZBI w taki sposób, aby właściwe adresować uprawnienia dostępu do polityk, procedur, instrukcji dla interesariuszy/grup interesariuszy SZBI za pomocą mechanizmów autoryzacji wg zasady „wiedzy koniecznej”,

3.4. Umożliwić wersjonowanie treści polityk, procedur, instrukcji,

3.5. Zapewnić dostęp do historii zmian,

3.6. Umożliwić wydruk polityk,

3.7. Posiadać wbudowany edytor treści polityk z możliwością bezpośredniej edycji diagramów stanowiących element opis dokumentacji na poziomie procedur, instrukcji,

3.8. Zapewnić możliwość linkowania treści serwisów informacyjnych stanowiących element bazy wiedzy SZBI.

4. Na potrzeby instalacji oferowanego oprogramowania Zamawiający udostępni Wykonawcy dedykowaną maszynę wirtualną z systemem MS Windows Server 2022 lub systemem operacyjnym z rodziny Linux klasy „open source".

3.3 Załącznik 3: Zakres testów bezpieczeństwa

1. Celem przeprowadzenia testów bezpieczeństwa jest identyfikacja słabych punktów systemu zabezpieczeń w infrastrukturze IT.
2. Do przeprowadzenia testów Wykonawca powinien wykorzystać metodyki blackbox i greybox stosujące przy tym manualne oraz automatyczne metody prowadzenia testów.
3. Zakres usługi w zakresie testów bezpieczeństwa musi obejmować, co najmniej:

3.1. detekcję podatności systemów obejmującą badania:

3.1.1. błędów w konfiguracji zabezpieczeń, umożliwiających nieuprawnione działanie;

3.1.2. potencjalnych możliwości nieuprawnionego dostępu do danych;

3.1.3. znanych podatności zidentyfikowanych systemów;

3.1.4. podatności typu SQL injection, XML injection etc.;

3.1.5. detekcja zabezpieczeń na podatność CSRF (Cross Site Request Forgery);

3.1.6. losowości ID sesji, sprawdzenie bezpieczeństwa budowy formularza logowania;

3.1.7. próby dostępu do zasobów bez uwierzytelnienia użytkownika (Authorization Bypass);

3.1.8. próby wykonania wrogiego kodu na serwerze (Code Execution);

3.1.9. podatności na ataki typu File Inclusion, Response Splitting, Deserialization of untrusted data;

3.2. testy środowiska web serwerów obejmujące m.in.:

3.2.1. bezpieczeństwo skonfigurowanego mechanizmu SSL;

3.2.2. dostępność komunikatów o błędach;

3.2.3. analizę podatności występujących w zainstalowanej wersji serwera;

3.2.4. dostępność nadmiarowych metod http;

3.3. analizę metod uwierzytelniania, w ramach którego wykonane zostaną w szczególności następujące czynności:

3.3.1. weryfikacja certyfikatów SSL;

3.3.2. weryfikacja kanałów komunikacyjnych;

3.3.3. ocenę zgodności z zaleceniami OWASP TOP10.

4. Wynikiem z testów jest opracowany przez Wykonawcę Raport z testów bezpieczeństwa, który powinien zawierać, co najmniej:

   4.1. udokumentowanie przeprowadzonych testów i ich rezultaty, w tym w szczególności wykryte podatności ze wskazaniem ich potencjalnego wpływu na bezpieczeństwo systemów i przetwarzanych w nim danych,

   4.2. wnioski, zalecenia i rekomendacje mające na celu usunięcie podatności i poprawę bezpieczeństwa.

5. W czasie realizacji zamówienia, w tym w szczególności w okresie prowadzonych testów bezpieczeństwa Wykonawca będzie odpowiedzialny wobec Zamawiającego za wszelkie swoje działania i zaniechania oraz działania i zaniechania swoich pracowników, podwykonawców i osób trzecich, którymi będzie posługiwał się przy realizacji tych zadań.

3.4 Załącznik 4: Szkolenia z zakresu bezpieczeństwa informacji

1. Wykonawca przeprowadzi szkolenia odrębnie w organizacji UMiG oraz OPS z zakresu bezpieczeństwa informacji odpowiednio do zdefiniowanych w SZBI ról oraz stanowisk pracy dla wszystkich stanowisk pracy (pracowników) objętych zasięgiem działania SZBI w UMiG oraz w OPS.

2. Zakres szkoleń dla każdej roli musi być uzgodniony z Zespołem ds. SZBI, gdzie punktem wyjścia do jego zdefiniowania, a przede wszystkim uszczegółowienia, odpowiednio do zakresu zadań i odpowiedzialności danej roli / stanowiska powinien być poniższy ogólny zakres zagadnień:

   2.1. Struktura i cele Systemu Zarządzania Bezpieczeństwem Informacji,

   2.2. Aspekt praktyczny wdrożenia SZBI, rola i odpowiedzialność kierownictwa oraz pracowników w jego funkcjonowaniu,

   2.3. Polityki i procedury związane z bezpieczeństwem informacji,

   2.4. Rodzaje i rozpoznawanie zagrożeń oraz ich wpływ na działalność organizacji,

   2.5. Konsekwencje zagrożeń związanych z ryzykiem utraty danych, naruszeniem bezpieczeństwa informacji,

   2.6. Ochrona danych i informacji, w tym podstawowe zasady ochrony danych osobowych i informacji wrażliwych, zgodnie z obowiązującymi przepisami (np. RODO) oraz metody i zastosowane techniki zabezpieczeń,

   2.7. Zasady bezpiecznego korzystania z infrastruktury IT oraz z systemów informatycznych,

   2.8. Reagowanie na incydenty bezpieczeństwa, w tym procedury zgłaszania incydentów bezpieczeństwa oraz sposoby ich dokumentowania,

   2.9. Metody ciągłego doskonalenia SZBI - audyty oraz działania korygujące

   2.10. Podnoszenie świadomości oraz kompetencji z zakresu bezpieczeństwa informacji jako proces przy pełnym udziale kierownictwa oraz pracowników w organizacji,

   2.11. Budowanie bazy wiedzy oraz promocja bezpieczeństwa informacji,

   2.12. Socjotechnika i „biały wywiad” w kontekście bezpieczeństwa informacji.