

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

na realizację zadania pn.

„Usługa wykonania audytu w ramach projektu Cyberbezpieczny Samorząd”**1. Wymagania ogólne**

- 1) Przedmiotem zamówienia jest Usługa wykonania audytu w ramach projektu Cyberbezpieczny Samorząd oraz opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji wraz z jej wdrożeniem.
- 2) Całość przedmiotu zamówienia musi być zrealizowana zgodnie z zapisami Specyfikacji Warunków Zamówienia.

2. Przedmiotem zamówienia jest Usługa wykonania audytu w ramach projektu Cyberbezpieczny Samorząd oraz opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji wraz z jej wdrożeniem dla poniżej wskazanych jednostek.

- 2.1. Urząd Miasta Rypin
- 2.2. Środowiskowy Dom Samopomocy
- 2.3. Miejski Ośrodek Sportu i Rekreacji w Rypinie
- 2.4. ZS-P nr 1, Szkoła Podstawowa Nr 1 im. Mjr. Henryka Sucharskiego
- 2.5. ZS-P nr 1, Przedszkole Miejskie nr 2 w Rypnie
- 2.6. ZS-P nr 1, Liceum Plastyczne w Rypinie
- 2.7. ZS-P nr 2, Szkoła Podstawowa nr 3 im. Jana Pawła II w Rypinie
- 2.8. ZS-P nr 2, Przedszkole Miejskie nr 1 w Rypnie
- 2.9. ZS-P nr 2, Przedszkole Miejskie nr 3 „Niezapominajka” w Rypnie
- 2.10. Miejski Zespół Obsługi Oświaty w Rypinie
- 2.11. Miejski Ośrodek Pomocy Społecznej w Rypinie
- 2.12. Centrum Aktywności Społecznej „KATOLIK”

3. Audyt wymagany w programie w zgodności z KRI – usługa przeprowadzenia 12 audytów zgodnie z Krajowymi Ramami Interoperacyjności oraz Ustawą o Krajowym Systemie Cyberbezpieczeństwa.

3.1. Zamawiający wymaga, aby audyty przeprowadzone przez Wykonawcę w 12 jednostkach Zamawiającego wykonywane były zgodnie z Krajowymi Ramami Interoperacyjności wraz z weryfikacją wszelkich niezbędnych elementów ujętych w Ustawie o Krajowym Systemie Cyberbezpieczeństwa w kontekście Systemu Zarządzania Bezpieczeństwem Informacji. Realizacja audytów w wymienionych obszarach ma pozwolić Zamawiającemu na kompleksową ocenę stanu bezpieczeństwa informacji oraz poziomu cyberbezpieczeństwa w Jednostkach, identyfikację potencjalnych luk i ryzyk. Zamawiający wymaga, aby audyty zostały zakończone sporządzeniem raportu zawierającego szczegółowe wyniki oraz rekomendacje dotyczące działań naprawczych i usprawniających.

3.2. Z uwagi na ilość Jednostek Zamawiający wymaga, aby usługa została przeprowadzona przez Wykonawcę posiadającego zespół audytorski, składający z audytorów wiodących, umożliwiający rzetelne wykonanie usługi. Zamawiający wymaga, aby na zespole audytorskim spoczywał obowiązek weryfikacji zgodności z innymi przepisami, w tym:

3.2.1. zgodność z przepisami dotyczącymi ochrony danych osobowych (np. RODO), w kontekście zarządzania danymi, bezpieczeństwa informacji oraz cyberbezpieczeństwa,

3.2.2. sprawdzenie zgodności z krajowymi i międzynarodowymi normami oraz standardami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem.

3.2.3. Zamawiający wymaga, aby wymienione wyżej audyty stanowiły jednocześnie audyt końcowy do projektu Cyberbezpieczny Samorząd i muszą zostać przeprowadzone przed ostatecznym rozliczeniem projektu oraz po wykonaniu i wdrożeniu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

3.2.4. Zamawiający określa także, że w ramach realizacji czynności audytowych, Wykonawca zobowiązany jest do przeprowadzenia testów penetracyjnych (rozumianych jako testy mające na celu identyfikację nieznanych podatności – wyłącznie skanowanie znanych podatności za pomocą narzędzi takich jak Nessus, OpenVAS (Greenbone), BurpSuite, Acunetix lub podobnych nie spełnia wymagań testów penetracyjnych), których minimalny zakres powinien obejmować:

3.2.4.1. Zewnętrzne testy penetracyjne infrastruktury IT, w tym:

- Analiza topologii styku z siecią Internet – ocena struktury oraz zabezpieczeń na granicy sieci lokalnej i Internetu.
- Weryfikacja mechanizmów ochronnych – analiza i testowanie systemów takich jak firewalle, IDS/IPS oraz inne zabezpieczenia na granicy sieci.
- Identyfikacja dostępnych usług sieciowych – skanowanie otwartych portów oraz publicznie dostępnych usług w celu wykrycia potencjalnych punktów dostępu.
- Analiza wersji oprogramowania dostępnego z Internetu – identyfikacja wersji i typów oprogramowania w celu wykrycia potencjalnych podatności.

- Eksploatacja wykrytych podatności – próby wykorzystania podatności urządzeń i usług wystawionych na zewnątrz w celu oceny ryzyka.
- Rekomendacje dotyczące bezpieczeństwa – opracowanie zaleceń poprawiających ochronę sieci lokalnej w kontekście jej styku z Internetem.

3.2.4.2. Wewnętrzne testy penetracyjne infrastruktury IT, w tym:

- Ocena topologii sieci LAN – analiza struktury oraz stosowanych zabezpieczeń sieci wewnętrznej.
- Weryfikacja zabezpieczeń sieciowych – ocena skuteczności mechanizmów ochronnych, segregacji i izolacji urządzeń w sieci lokalnej.
- Analiza ruchu sieciowego – monitoring i analiza w poszukiwaniu anomalii mogących świadczyć o naruszeniach bezpieczeństwa.
- Identyfikacja usług i hostów sieciowych – skanowanie portów, wykrywanie usług oraz analiza aktywnych urządzeń w sieci wewnętrznej.
- Eksploatacja podatności wewnętrznych – testy mające na celu ocenę potencjalnych ryzyk wynikających z luk w sieci LAN.
- Ocena procedur backupu – analiza procesów tworzenia i odtwarzania kopii zapasowych.
- Monitorowanie bezpieczeństwa – weryfikacja systemów monitorowania pod kątem wykrywania zagrożeń i incydentów.
- Rekomendacje dotyczące bezpieczeństwa sieci LAN – propozycje poprawy zabezpieczeń infrastruktury wewnętrznej.

3.2.4.3. Audyt serwisów WWW obejmujący:

- Weryfikację wersji serwera HTTP i systemu CMS – sprawdzenie ich aktualności i podatności na znane zagrożenia.
- Analizę bezpieczeństwa komunikacji – ocena certyfikatów X.509, wersji protokołu TLS oraz stosowanych algorytmów kryptograficznych.

3.2.4.4. Audyt serwisów pocztowych obejmujący:

- Mechanizmy SPF, DKIM i DMARC – ocena poprawności ich wdrożenia w celu zapobiegania spoofingowi i zwiększenia zaufania do wiadomości e-mail.
- Bezpieczeństwo TLS w komunikacji pocztowej – analiza poprawności konfiguracji i bezpieczeństwa mechanizmów szyfrowania.

3.2.4.5. Raport końcowy z testów i audytów:

- Opis zakresu i metodologii prac – szczegółowe przedstawienie użytych narzędzi, technik oraz analizowanych obszarów.
- Analiza wyników – prezentacja zidentyfikowanych podatności oraz ich potencjalnych konsekwencji.
- Rekomendacje naprawcze – propozycje działań zwiększających bezpieczeństwo oraz strategii minimalizacji ryzyk.
- Weryfikacja aspektów technicznych – szczegółowa analiza zabezpieczeń serwisów WWW, pocztowych, lokalnych sieci oraz połączeń z Internetem, wraz z zaleceniami dotyczącymi utrzymania wysokiego poziomu ochrony.

4. Aktualizacja – wdrożenie SZBI – usługa opracowania i wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji

4.1. Zamawiający wymaga, aby usługa przeprowadzona została przez Wykonawcę w 12 wyżej wskazanych jednostkach.

4.2. Zakres dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji musi obejmować kompleksowe opracowanie polityk, procedur i wytycznych, które pozwolą na skuteczne zarządzanie bezpieczeństwem informacji w oparciu o obowiązujące przepisy prawa oraz normy, takie jak ISO/IEC 27001 i ISO/IEC 22301. Dokumentacja ma na celu nie tylko spełnienie formalnych wymagań, ale przede wszystkim zapewnienie realnej ochrony przetwarzanych danych oraz kluczowych zasobów Jednostek.

4.3. Zakres prac musi obejmować określenie zasad zarządzania ryzykiem, które pozwolą na identyfikację i minimalizację potencjalnych zagrożeń dla poufności, integralności oraz dostępności informacji. W dokumentacji muszą się znaleźć również szczegółowe wytyczne dotyczące bezpieczeństwa fizycznego, takie jak ochrona dostępu do budynków i pomieszczeń, a także zasady zabezpieczania sprzętu i infrastruktury IT. Opracowane muszą zostać procedury ciągłości działania dla zapewnienia przygotowania Jednostek na ewentualne zakłócenia w pracy, umożliwiając szybkie przywrócenie kluczowych procesów operacyjnych.

4.4. Integralną częścią dokumentacji muszą być również procedury reagowania na incydenty, w tym mechanizmy monitorowania i raportowania naruszeń bezpieczeństwa, a także działania naprawcze minimalizujące skutki ewentualnych zagrożeń. Wypracowane muszą zostać także zasady zarządzania dostępem, regulujące przyznawanie, weryfikację i cofanie uprawnień do systemów oraz danych.

4.5. Dokumentacja musi uwzględniać również elementy związane z podnoszeniem świadomości pracowników, obejmujące szkolenia, tj. wymaga się, aby Wykonawca w dokumentacji określił również harmonogramy szkoleń i obszary, dla których wymaga się przeprowadzenia przez Zamawiającego odrębnych szkoleń dla pracowników i kadry Jednostek.

4.6. Zamawiający wymaga, aby całość dokumentacji została przygotowana w sposób zintegrowany, co ma zapewnić spójność i efektywność systemu zarządzania bezpieczeństwem informacji w 12 Jednostkach oraz jego dostosowanie do specyfiki działania Jednostek.

4.7. Zamawiający w ramach usługi opracowania dokumentacji wymaga również od wykonawcy dostarczenia dla Urzędu Miasta Rypin aplikacji/oprogramowania, która pozwoli wspomagać systemowe zarządzanie Urzędem (wyłącznie dla Urzędu Miasta Rypin) w zakresie bezpieczeństwa informacji i ochrony danych osobowych.

4.7.1. Zamawiający określa szczególne wymagania ogólne dla aplikacji/oprogramowania

- Oprogramowanie ma być dostarczone w najnowszej wersji w języku polskim.
- Oprogramowanie musi posiadać dokumentację użytkownika opisującą funkcjonalność każdego z modułów oprogramowania oraz dokumentację administratora opisującą sposób administrowania programem w tym jego instalowania, konfiguracji, sposobu tworzenia kopii zapasowych oraz odtwarzania w przypadku awarii.
- Program powinien umożliwiać pracę zarówno na komputerach stacjonarnych jak i na urządzeniach mobilnych np. smartfonach.
- Program na komputerze klienckim powinien posiadać możliwość instalacji jako aplikacja PWA.

- Koszt zakupu oprogramowania powinien uwzględniać koszt wszystkich składników oprogramowania (poza systemem operacyjnym zainstalowanym na serwerze Zamawiającego), które są niezbędne do jego pracy zgodnie z niniejszą specyfikacją.
- W ramach zamówienia Zamawiający musi otrzymać wersję instalacyjną oprogramowania oraz licencję uprawniającą do korzystania z przedmiotowego oprogramowania.

4.7.2. Techniczne dane oprogramowania

- Program powinien pracować jako aplikacja intranetowa uruchamiana i prawidłowo pracująca w aktualnych wersjach przeglądarek internetowych (MS Edge, Google Chrome, FireFox).
- Wszystkie dane gromadzone w oprogramowaniu powinny być zapisywane wyłącznie centralnie, na komputerze pełniącym rolę serwera pracującego w trybie ciągłym przez 24 godziny na dobę.
- Serwer będzie dostarczony przez Zamawiającego i będzie znajdował się w jego siedzibie.
- Program powinien pracować na serwerze z procesorem 8-rdzeniowy w architekturze 64 bit., min. 1TB SSD, min. 16GB RAM z zainstalowanym systemem operacyjny Windows lub Linux (inne składniki oprogramowania niezbędne do pracy programu dostarcza Dostawca).
- Aplikacja instalowana na serwerze działającym w systemie Windows powinna posiadać automatyczny instalator wszystkich składników niezbędnych do prawidłowego działania oprogramowania.
- Poza instalatorem dla systemu Windows aplikacja powinna mieć możliwość uruchomienia na serwerze pracującym pod systemem Linux (konfiguracja instalacji niestandardowych powinna być określona w dokumentacji programu).
- Program ma mieć możliwość importu użytkowników z przygotowanego zgodnie ze specyfikacją pliku lub ich importu bezpośrednio z Active Directory.
- Program ma mieć możliwość opcjonalnej integracji z Active Directory.

4.7.3. Funkcjonalność oprogramowania i jego zakres działania

Specjalistyczne oprogramowanie do zarządzania urzędem w zakresie m.in. bezpieczeństwa informacji i ochrony danych osobowych musi posiadać funkcjonalności, które umożliwiają zarządzanie obszarami m.in.:

4.7.3.1. Procesami realizowanymi w Urzędzie – w tym zakresie oprogramowanie musi:

- posiadać rejestr zidentyfikowanych procesów w tym procesów z zakresu ochrony danych, który umożliwia ich podział na makroprocesy,
- posiadać możliwość opisu procesu poprzez określenie początku i końca procesu, danych wejściowych i wyjściowych procesu, dostawcę, klienta procesu, zakresu podmiotowego i przedmiotowego, dokumentów wymaganych w procesie oraz ryzyk wpływających na osiągnięcie celu procesów,
- posiadać graficzny edytor do tworzenia interaktywnych map procesów (z możliwością podpinania plików pod dowolne elementy grafu),

4.7.3.2. Komórkami organizacyjnymi – w tym zakresie oprogramowanie musi:

- posiadać rejestr komórek organizacyjnych, który będzie oparty na zatwierdzonym w Urzędzie regulaminie organizacyjnym,
- posiadać możliwość opisu komórki organizacyjnej poprzez określenie jej podrzędności w strukturze organizacyjnej, przypisania do niej stanowisk pracy oraz zakresu zadań jaki realizuje,

4.7.3.3. stanowiskami pracy – w tym zakresie oprogramowanie musi:

- posiadać rejestr stanowisk pracy przypisanych do właściwych komórek organizacyjnych, zgodnie z obowiązującym regulaminem organizacyjnym,
- posiadać możliwość opisu stanowiska pracy poprzez określenie m.in.: miejsca stanowiska pracy w strukturze organizacyjnej, celu istnienia stanowiska pracy, liczby podległych pracowników, głównych zadań realizowanych na stanowisku pracy, wymaganych upoważnień i pełnomocnictw obowiązujących na danym stanowisku pracy oraz wymaganiach w zakresie kompetencji czy doświadczenia,

4.7.3.4. pracownikami – w tym zakresie oprogramowanie musi:

- posiadać rejestr wszystkich pracowników, praktykantów i stażystów oraz osób świadczących pracę na umowach cywilnoprawnych,
- posiadać możliwość prześledzenia historii zatrudnienia pracownika, w zakresie m.in. obejmowanych stanowisk pracy, pełnionych przez niego funkcji i posiadanych uprawnień w aplikacjach przez niego eksploatowanych w organizacji,

4.7.3.5. dokumentami – w tym zakresie oprogramowanie musi:

- posiadać rejestr wszystkich dokumentów określających wymagania (m.in.: polityk, zarządzeń, decyzji, instrukcji, procedur) obowiązujących na poszczególnych stanowiskach pracy w urzędzie,
- posiadać możliwość opisu dokumentu poprzez m.in.: określenie osoby odpowiedzialnej za dokument, przypisanie do procesu, który realizuje oraz wskazanie właściwych stanowisk pracy na jakich obowiązuje,
- posiadać możliwość udostępniania treści dokumentu pracownikom,
- posiadać możliwość elektronicznego wnioskowania o utworzenie bądź zmianę dokumentu, nadzorowania etapów jego tworzenia oraz opiniowania przez wytypowanych użytkowników przestanego projektu dokumentu,
- posiadać możliwość dystrybucji zatwierdzonego dokumentu na stanowiska pracy, na których obowiązuje dokument,
- posiadać możliwość elektronicznego zapoznania się przez użytkownika, będącego jednocześnie pracownikiem urzędu, z dokumentem obowiązującym na zajmowanym przez niego stanowisku pracy i elektronicznego potwierdzenia zapoznania się z treścią dokumentu,
- posiadać narzędzia weryfikacji danych dotyczących potwierdzenia zapoznania pracowników z dokumentacją obowiązującą na ich stanowisku pracy,

4.7.3.6. założeniami wdrożonego w Urzędzie SZBI – w tym zakresie oprogramowanie musi:

- wspomagać opisywanie kontekstu organizacji w tym dokumentować okresowe analizy czynników mających wpływ na zdolność organizacji do osiągnięcia zamierzonych celów, umożliwiać opisanie zakresu i wyłączeń systemu oraz potrzeb i oczekiwań stron zainteresowanych,
 - udostępniać pracownikom przygotowaną w programie deklarację polityki bezpieczeństwa informacji wraz ze spójnymi z nią celami powiązаныmi z procesami oraz wskaźnikami ich pomiarów,
 - w sposób przejrzysty udostępniać pracownikom organizacji pełne wymagania systemu zarządzania bezpieczeństwem informacji i ochrony danych osobowych, w tym prezentować w formie graficznej wzajemne powiązania dokumentacji (tworzyć interaktywny schemat z możliwością otwierania poszczególnych dokumentów po kliknięciu na elementy grafu).
- 4.7.3.7. sprzętem komputerowym i oprogramowaniem komputerowym – w tym zakresie oprogramowanie musi:
- posiadać rejestr wszystkich urządzeń informatycznych oraz zainstalowanego na nim oprogramowania komputerowego,
 - mieć możliwość automatycznego odczytywania parametrów sprzętowych i oprogramowania zainstalowanego na komputerach działających pod kontrolą systemu operacyjnego Windows,
 - posiadać możliwość ewidencjonowania bieżących przeglądów sprzętu komputerowego oraz zainstalowanego na nim oprogramowania,
 - posiadać możliwość elektronicznego zgłaszania usterek i awarii sprzętu komputerowego,
 - posiadać możliwość ewidencjonowania rodzaju umów serwisowych na sprzęt komputerowy,
 - posiadać możliwość ewidencjonowania i zarządzania materiałami eksploatacyjnymi niezbędnymi do pracy sprzętów komputerowych np. tonery do drukarek,
 - posiadać możliwość ewidencji wszystkich zdarzeń, czynności naprawczych, serwisowych czy konserwacyjnych komputerów lub serwera.
- 4.7.3.8. licencjami na oprogramowanie – w tym zakresie oprogramowanie musi:
- posiadać rejestr licencji oprogramowania komputerowego zainstalowanego na komputerach w Urzędzie oraz rejestr umów licencyjnych podpisanych przez Urząd na dostawę specjalistycznego oprogramowania,
 - posiadać możliwość ewidencji posiadanych przez Urząd umów na korzystanie z licencji programów komputerowych,
- 4.7.3.9. obsługą problemów zgłaszanych przez użytkowników – w tym zakresie oprogramowanie musi:
- dostarczać użytkownikom kanał komunikacji do zgłaszania problemów z obszaru IT,
 - dokumentować obsługę zgłoszeń oraz nadzorować terminowości ich realizacji,
 - określać kategorie zgłoszeń i ustalać osoby odpowiedzialne za ich obsługę,
- 4.7.3.10. aktywami informacyjnymi – w tym zakresie oprogramowanie musi:
- umożliwiać prowadzenie rejestru zidentyfikowanych aktywów informacyjnych oraz zasobów wspomagających,

- wspomagać opisywanie aktywów m.in. poprzez wskazanie procesów przetwarzających informacje oraz istotności informacji dla realizacji danego procesu, wskazanie zasobów wykorzystywanych przy przetwarzaniu informacji oraz określenie poziomu istotności zasobu dla informacji,
- umożliwiać ustalenie wymaganego poziomu podstawowych oraz dodatkowych atrybutów informacji i adekwatnie do tego ustalać klasyfikacje aktywów.

4.7.3.11. ochrony danych osobowych – w tym zakresie oprogramowanie musi:

- umożliwiać prowadzenie zgodnie z przepisami prawa rejestru czynności przetwarzania i kategorii czynności przetwarzania danych osobowych w Urzędzie,
- posiadać możliwość rejestrowania klauzul informacyjnych udostępnianych przez Urząd, a w przypadku klauzul kierowanych do pracowników program automatycznie informuje pracowników o konieczności zapoznania się z klauzulą informacyjną i udostępnia użytkownikom uprawnionym informacje o dacie zapoznania się pracowników z poszczególnymi klauzulami informacyjnymi,
- posiadać możliwość ewidencji zawartych przez Urząd umów powierzenia przetwarzania danych osobowych,
- wspomagać wystawianie upoważnień do przetwarzania danych osobowych oraz prowadzić rejestr osób upoważnionych do przetwarzania danych osobowych,
- posiadać elektroniczny rejestr udostępnionych danych osobowych, który zawiera m.in. informacje o wnioskującym, dacie wniosku, podstawie prawnej upoważniającej do udostępnienia danych, zakresie udostępnionej informacji oraz terminie i osobie udostępniającej,
- umożliwiać ewidencjonowanie oraz wspomagać obsługę wniosków wynikających z RODO tj.: dostęp do danych osobowych (art. 15 RODO), sprostowanie danych osobowych (art. 16 RODO), usunięcie danych osobowych (art. 17 RODO), ograniczenie przetwarzania danych osobowych (art. 18 RODO), przeniesienie danych osobowych (art. 20 RODO), sprzeciw wobec przetwarzania danych osobowych (art. 21 RODO),

4.7.3.12. zarządzaniem ryzykiem bezpieczeństwa informacji – w tym zakresie oprogramowanie musi:

- posiadać rejestr zidentyfikowanych ryzyk w zakresie m.in. bezpieczeństwa informacji i ochrony danych osobowych,
- posiadać możliwość przypisania stanowiska odpowiedzialnego za zidentyfikowane ryzyko i jego cyklicznej oceny,
- posiadać możliwość identyfikacji i ewidencji czynników ryzyka (źródeł zagrożeń i szans), podatności na zagrożenia lub szanse, opisanie skutków ryzyka, estymację i ocenę ryzyka, ustalenia reakcji na ryzyko oraz monitorowania i raportowania ryzyka,
- posiadać możliwość przeprowadzania cyklicznej oceny ryzyka,
- prezentować ryzyka w formie graficznych zestawień m.in. mapy ryzyka,

4.7.3.13. zarządzania uprawnieniami użytkowników w aplikacjach – w tym zakresie oprogramowanie musi:

- posiadać rejestr wszystkich aplikacji użytkowanych w Urzędzie,

- posiadać rejestr nadanych w Urzędzie uprawnień do przetwarzania danych w aplikacjach komputerowych zgodnie z zakresem zadań wykonywanych przez pracownika,
- posiadać możliwość elektronicznego wnioskowania o nadanie właściwych uprawnień dla pracowników zgodnie z ich zakresem obowiązków do obsługi programów komputerowych, w których są przetwarzane dane osobowe,
- w przypadku aplikacji przetwarzających dane osobowe weryfikować czy pracownik posiada upoważnienie do przetwarzania danych osobowych,
- ustalać etapy przetwarzania wniosku m.in. akceptację, opiniowanie zatwierdzanie,
- informować użytkowników odpowiedzialnych za realizację danego etapu przetwarzania wniosku o konieczności jego zrealizowania,
- posiadać możliwość elektronicznego potwierdzenia przez pracownika zapoznania się z zakresem nadanego uprawnienia,

4.7.3.14. incydentami i słabościami systemu – w tym zakresie oprogramowanie musi:

- posiadać rejestr zaistniałych incydentów oraz słabości systemu,
- posiadać możliwość zgłoszenia zidentyfikowanego zdarzenia lub słabości systemu bezpieczeństwa informacji (w tym naruszenia ochrony danych osobowych),
- umożliwiać analizę i klasyfikację zgłoszonego zdarzenia,
- wspomagać obsługę incydentów bezpieczeństwa informacji w tym określenia operatora incyduentu oraz ewidencjonować podejmowane działania,
- posiadać stosowne zestawienia dotyczące zidentyfikowanych incydentów i słabości systemów w Urzędzie,

4.7.3.15. certyfikatami bezpieczeństwa – w tym zakresie oprogramowanie musi:

- posiadać rejestr certyfikatów bezpieczeństwa,
- posiadać możliwość wnioskowania o nadanie certyfikatu bezpieczeństwa,
- umożliwiać użytkownikom uprawnionym ewidencjonowanie certyfikatów bezpieczeństwa,
- umożliwiać elektroniczne potwierdzenia posiadania przez pracownika certyfikatu bezpieczeństwa,
- informować użytkowników uprawnionych o zbliżającym się terminie ważności certyfikatu i nadzorować etapy jego odnowienia,
- posiadać możliwość unieważniania certyfikatu bezpieczeństwa,

4.7.3.16. wewnętrznymi audytami w zakresie bezpieczeństwa informacji i ochroną danych osobowych – w tym zakresie oprogramowanie musi:

- posiadać rejestr przeprowadzonych w Urzędzie audytów wewnętrznych w tym auditów w zakresie bezpieczeństwa informacji i ochrony danych osobowych,

- posiadać możliwość tworzenia programów auditów wewnętrznych na dany rok oraz planowania auditów z określeniem m.in.: zakresu auditu, przedmiotu auditu, komórek organizacyjnych uczestniczących w działaniach auditowych, terminu przeprowadzenia auditu oraz osób przeprowadzających audit,
- możliwość dokumentowania podjętych działań auditowych tj. przygotowanie m.in.: programu auditów na dany rok, protokołu końcowego z auditu,
- możliwość dokumentowania wszystkich spostrzeżeń, niezgodności i wniosków wynikłych podczas podjętych działań auditowych,
- możliwość zgłoszenia zauważonych podczas auditu niezgodności do właściwej osoby odpowiedzialnej,

4.7.3.17. działaniami doskonalącymi – w tym zakresie oprogramowanie musi:

- posiadać rejestr wszystkich zidentyfikowanych w Urzędzie nieprawidłowości (niezgodności) w zakresie bezpieczeństwa informacji i ochrony danych osobowych,
- posiadać możliwość elektronicznego zgłaszania zidentyfikowanych nieprawidłowości w funkcjonowaniu systemu bezpieczeństwa informacji i ochrony danych osobowych,
- możliwość analizy zgłoszonej nieprawidłowości przez osoby za to odpowiedzialne,
- możliwość określenia działań korygujących i korekcyjnych względem zidentyfikowanej nieprawidłowości oraz głoszenia wykonania działań korygujących,

4.7.3.18. przeglądami zarządzania w zakresie bezpieczeństwa informacji i ochroną danych osobowych – w tym zakresie oprogramowanie musi:

- posiadać rejestr przeprowadzanych w Urzędzie cyklicznych przeglądów zarządzania w zakresie m.in. bezpieczeństwa informacji i ochrony danych osobowych,
- możliwość automatycznego przygotowania raportu do analizy z zakresu m.in. bezpieczeństwa informacji i ochrony danych osobowych.

4.7.4. Wszystkie moduły programu muszą być ze sobą kompatybilne i wzajemnie powiązane (moduły powinny korzystać z danych wprowadzanych w innych modułach bez konieczności ponownego ewidencjonowania tych samych danych).

4.7.5. Program musi informować użytkownika o działaniach, które musi podjąć w aplikacji ze względu na posiadane w aplikacji uprawnienia lub zajmowane w organizacji stanowisko pracy.

4.7.6. Komunikaty adresowane do użytkowników muszą być dostępne po zalogowaniu użytkownika do bezpośrednio aplikacji i w formie powiadomień PUSH oraz równolegle wysyłane na adres e-mail użytkownika.

4.7.7. Z poziomu komunikatu przesłanego pocztą elektroniczną użytkownik może przejść bezpośrednio do modułu w programie, w którym musi podjąć działania.

4.7.8. Licencja

4.7.8.1. Licencja ma być przyznana na czas nieograniczony wraz ze wsparciem autorskim do 21.06.2026 roku w trybie 5x8 h.

4.7.8.2. Licencja ma zezwalać na jednoczesną pracę w programie wszystkich pracowników Urzędu.

4.7.8.3. Licencja nie może ograniczać liczby końcówek jednocześnie korzystających z oprogramowania.

4.7.8.4. Licencja musi dopuszczać tworzenie przez Zamawiającego dowolnej ilości kopii oprogramowania dla celów testowych lub szkoleniowych.