*Załącznik nr 5 do zapytania ofertowego z dnia 25.03.2023 r*

**OPIS OFEROWANEGO PRZEDMIOTU ZAMÓWIENIA**

1. **Oprogramowanie do zarządzania ryzykiem**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Minimalny zakres wymagań, który powinien**  **spełniać oferowany przedmiot zamówienia** | **Parametry oferowanego przedmiotu zamówienia,**  **wartość parametru bądź potwierdzenie**  **spełniania wymaganych parametrów poprzez**  **wpisanie „TAK”** |
| 1 | **Funkcjonalności w obszarze organizacyjnym** | |
| odwzorowanie schematu organizacyjnego Zamawiającego |  |
| odwzorowanie procesów zachodzących w Starostwie |  |
| korelację procesów z komórkami organizacyjnymi Starostwa |  |
| korelację procesów ze zidentyfikowanymi ryzykami |  |
| korelację ryzyk z grupami ryzyka |  |
| wskazanie krytyczności procesu |  |
| wskazanie typów danych osobowych przetwarzanych w procesie |  |
| wskazanie szczególnych kategorii danych osobowych |  |
| możliwość przypisania regulacji do ryzyk |  |
| możliwość kontroli zaleceń audytowych |  |
| możliwość kontroli terminów wdrożeń zaleceń audytowych |  |
| możliwość kontroli ryzyk wymagających okresowych przeglądów |  |
| 2 | **Identyfikacja ryzyka w obszarach** | |
| środowiska teleinformatycznego |  |
| kontroli dostawców usług informatycznych |  |
| zarządzania kadrami |  |
| zarządzania bezpieczeństwem fizycznym |  |
| produktów i usług, w tym usług chmurowych |  |
| 3 | **Ocena ryzyka w zakresie** | |
| prawdopodobieństwa jego wystąpienia |  |
| skutków finansowych |  |
| skutków wizerunkowych |  |
| utraty poufności |  |
| utraty dostępności |  |
| utraty integralności |  |
| dodatkowych atrybutów definiowanych przez Zamawiającego |  |
| 4 | **Ocena DPIA (Data Protection Impact Assessment)** | |
| przypisanie negatywnych skutków do ryzyka |  |
| ocena skutków dla ochrony danych |  |
| dedykowany raport DPIA. |  |
| 5 | **Plan postępowania z ryzykiem** | |
| przypisanie priorytetu postępowania do planu |  |
| przypisanie osoby odpowiedzialnej |  |
| określenie kosztów |  |
| wskazanie terminu wprowadzenia planu |  |
| 6 | **Kluczowe Wskaźniki Ryzyka (Key Risc Indicators – KRI)** | |
| monitorowania ryzyka za pomocą KRI |  |
| mechanizm rejestracji pomiarów |  |
| alarmowanie o wskaźnikach wymagających pomiaru |  |
| raportowanie wyników |  |
| 7 | **Rejestr incydentów** | |
| możliwość rejestracji incydentów |  |
| przeprowadzanie szczegółowych analiz |  |
| monitorowanie wpływu na inne procesy |  |
| szacowanie potencjalnych strat i rejestrowanie strat rzeczywistych |  |
| kontrola czasu zgłoszenia naruszenia danych osobowych do UODO |  |
| dodawanie załączników (np. raportów notatek, zrzutów ekranowych) |  |
| 8 | Dostęp w jednym czasie dla 5 użytkowników Zamawiającego |  |
| 9 | Możliwość rozszerzenia o dodatkowe konta dostępu |  |
| 10 | Dostęp do bazy predefiniowanych ryzyk online (Internet) |  |
| 11 | Tworzenie nielimitowanej ilości identyfikowanych ryzyk |  |
| 12 | Importowanie i eksportowanie danych w formacie Excela |  |
| 13 | Licencja wieczysta |  |
| 14 | Instalacja w infrastrukturze Zamawiającego w modelu klient-serwer |  |
| 15 | Wsparcie podczas instalacji i konfiguracji bazy danych |  |
| 16 | Min. 6 – godzinne szkolenie dla osób wyznaczonych przez Zamawiającego z metodyki oraz pracy z wykorzystaniem narzędzia wspomagającego analizę ryzyka. |  |
| 15 | **Minimalne wymagania dla serwera** | |
| 200 MB przestrzeni dyskowej |  |
| 1 GB pamięci RAM |  |
| procesor 1Ghz |  |
| system Linux z zainstalowanym serwerem baz danych Firebird 3.0 |  |
| 16 | **Minimalne wymagania dla stacji roboczej** | |
|  | Windows 10 lub11 |  |
| 200 MB przestrzeni dyskowej |  |
| 1 GB pamięci RAM |  |
| procesor 1Ghz |  |
| 17 | Nazwa oferowanego oprogramowania, wersja, nazwa producenta. |  |

1. **wykonanie analizy ryzyka dla Starostwa Powiatowego w Świdnicy**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Minimalny zakres wymagań, który powinien**  **spełniać oferowany przedmiot zamówienia** | **Parametry oferowanego przedmiotu zamówienia,**  **wartość parametru bądź potwierdzenie**  **spełniania wymaganych parametrów poprzez**  **wpisanie „TAK”** |
| 1 | dokonanie oceny zabezpieczeń technicznych i organizacyjnych stosowanych przez Zamawiającego |  |
| 2 | opracowanie raportu bezpieczeństwa na podstawie przeprowadzonej oceny stosowanych przez Zamawiającego zabezpieczeń technicznych i organizacyjnych |  |
| 3 | identyfikacja ryzyk w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji, w tym ochrony danych osobowych. |  |
| 4 | ocena co najmniej 100 ryzyk |  |
| 5 | wykonanie DPiA – oceny skutków dla ochrony danych osobowych przetwarzanych przez Zamawiającego |  |
| 6 | przygotowanie planów postępowania z ryzykiem |  |

1. **Przygotowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Minimalny zakres wymagań, który powinien**  **spełniać oferowany przedmiot zamówienia** | **Parametry oferowanego przedmiotu zamówienia,**  **wartość parametru bądź potwierdzenie**  **spełniania wymaganych parametrów poprzez**  **wpisanie „TAK”** |
| 1 | **Polityka Bezpieczeństwa Teleinformatycznego** | |
| zasady korzystania z systemów informatycznych |  |
| procedury zmiany uprawnień |  |
| instrukcja wykonywania kopii zapasowej |  |
| instrukcja odtworzenia kopii zapasowej |  |
| rejestr komponentów bez wsparcia producentów |  |
| protokół przekazania sprzętu do naprawy |  |
| zarządzanie konfiguracją |  |
| wzorce konfiguracji |  |
| rejestr komponentów środowiska teleinformatycznego |  |
| listę parametrów wydajności i pojemności systemów teleinformatycznych |  |
| zasady zapisów do raportów monitorowania wydajności i pojemności systemów teleinformatycznych Zamawiającego |  |
| zasady zapisów do raportów monitorowania usług zewnętrznych |  |
| instrukcja wycofania komponentów teleinformatycznych |  |
| zasady prowadzenia audytu wewnętrznego systemów teleinformatycznych |  |
| procedury monitorowania i przeglądu systemów teleinformatycznych |  |
| zasady wprowadzania i wyprowadzania danych do systemów teleinformatycznych |  |
| zasady szkolenia użytkowników systemów teleinformatycznych |  |
| 2 | **Polityka Bezpieczeństwa Informacji** | |
| deklaracja stosowania |  |
| odwołania do innych aktów wewnętrznych Zamawiającego, dotyczących bezpieczeństwa przetwarzania informacji (np. Polityka przetwarzania danych osobowych w Starostwie Powiatowym w Świdnicy, Instrukcja zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych w Starostwie Powiatowym w Świdnicy, szczególne Wymagania Bezpieczeństwa oraz Procedury Bezpiecznej Eksploatacji dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych, itp.) |  |
| rejestr wymaganych definicji |  |
| przypisanie odpowiedzialności i ról w zakresie utrzymywania SZBI. |  |
| Polityka Klasyfikacji Informacji |  |
| Polityka Klasyfikacji Systemów Informatycznych, |  |
| opis metodyki szacowania ryzyka |  |
| raport z procesu szacowania ryzyka |  |
| plan postępowania z ryzykiem |  |
| zasady zarządzania incydentami bezpieczeństwa |  |
| zasady zarządzania rejestrem wyjątków od PBI |  |
| monitorowanie i przegląd SZBI |  |
| 4 | **Zarządzanie dostawcami usług informatycznych** | |
| wzory klauzul do umów z dostawcami |  |
| przykładowe porozumienie o poufności |  |
| zasady zwrotu informacji |  |
| rejestr umów zawartych z dostawcami zewnętrznymi |  |
| przegląd umowy i ocena dostawcy usługi |  |
| 5 | **Planu Ciągłości Działania (PCD)** | |
| wdrożenie dla jednego procesu krytycznego zgodnie z normą ISO 22301. |  |
| szkolenia/warsztaty dla osób odpowiedzialnych za nadzorowanie PCD |  |
| przekazanie wzorcowej dokumentacji (wprowadzenie, klasyfikacja, zarządzanie incydentami i analiza ryzyka) |  |
| Wsparcie przy identyfikacji i klasyfikacji kluczowych procesów ( BCP – Business Continuity Planning) |  |
| wsparcie przy analizie ryzyka / scenariuszach utraty ciągłości działania |  |
| wsparcie przy zarządzaniu incydentami |  |
| weryfikacja wdrożenia zarządzania incydentami, klasyfikacji procesów i analizy ryzyka |  |
| szkolenie osób odpowiedzialne za nadzorowanie PCD (opracowywanie Minimalnych Akceptowalnych Konfiguracji - MAK-ów), |  |
| wsparcie przy adaptacji dokumentacji PCD (uzupełnienie kontaktów, uzupełnienie treści komunikatów, uzupełnienie personelu i zasobów sprzętowych) |  |
| wsparcie przy przygotowaniu MAK |  |
| weryfikacja dokumentacji PCD i MAK |  |
| wsparcie przy przygotowaniu instrukcji odtworzeniowych (odtwarzanie serwerów, urządzeń wirtualnych, instrukcja przełączenia) |  |
| testowanie planów, weryfikacja instrukcji odtworzeniowych oraz wykonanie raportu z testów. |  |

W załączniku zawarto minimalne wymagania, co oznacza, że Wykonawca może zaoferować przedmiot zamówienia charakteryzujący się większym zakresem prac ww. zagadnień.

UWAGA: Niespełnienie wymagań minimalnych będzie skutkować odrzuceniem oferty.

**……………………………………………….**

**Data, Podpis Wykonawcy**