

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest opracowanie, aktualizacja i wsparcie podczas wdrożenia **Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Ekosystem Sp. z o.o.**
2. W ramach zamówienia Wykonawca:
 - 1) opracuje dokumentację SZBI, która obejmie organizację Zamawiającego z wyłączeniem obszaru przetwarzania informacji niejawnych w rozumieniu ustawy o ochronie informacji niejawnych, zgodnie z przepisami prawa w zakresie Krajowego Systemu Cyberbezpieczeństwa oraz Ochrony Danych Osobowych, wraz z przekazaniem praw autorskich do dokumentacji,
 - 2) będzie świadczył usługi konsultacyjne, doradcze, prace analityczne.
3. Na zakres prac realizowanych przez Wykonawcę w ramach opracowania, aktualizacji i wsparcia podczas wdrożenia SZBI składają się co najmniej:
 - 1) Wykonanie oceny obecnej dostępnej dokumentacji,
 - 2) Określenie stanu faktycznego zabezpieczeń danych w systemach informatycznych poprzez przeprowadzenie audytu zabezpieczeń dostępu do danych oraz przygotowanie raportu wraz z zaleceniami i projektem zmian, spełnienie wymagań normy PN-EN ISO/IEC 27001:2023 i zaleceń norm pokrewnych, oraz wymagań prawnych nałożonych na organizację, między innymi dotyczących ochrony danych osobowych,
 - 3) Przeprowadzenie instruktażu wprowadzającego dla pracowników w zakresie ochrony informacji, inwentaryzacji aktywów informacyjnych oraz oceny ryzyka,
 - 4) Opracowanie Polityki Bezpieczeństwa zgodnej z wymaganiami normy PN-EN ISO/IEC 27001:2023 i zaleceń norm pokrewnych, oraz wymagań prawnych nałożonych na organizację, między innymi dotyczących ochrony danych osobowych w zakresie:
 - a) organizacja systemu bezpieczeństwa informacji,
 - b) zarządzanie aktywami,
 - c) zarządzania zasobami ludzkimi,
 - d) organizacja bezpieczeństwa fizycznego i środowiskowego,
 - e) zarządzanie komunikacją i eksploatacją,
 - f) rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania,
 - g) kontrola dostępu, zarządzania hasłami, stosowania zabezpieczeń kryptograficznych, czystego biurka i czystego ekranu, usuwania i niszczenia informacji, pracy w strefach bezpieczeństwa,
 - h) akwizycja, rozwój i utrzymanie systemu,
 - i) zarządzanie incydentami związanymi z bezpieczeństwem informacji,
 - j) zarządzanie ciągłością działania,
 - k) zarządzanie kopiami zapasowymi,
 - l) zarządzanie monitoringiem,
 - m) zobowiązanie do zachowania poufności, stosowania polityk i procedur SZBI,
 - n) używania urządzeń komputerowych,
 - o) metoda szacowania i postępowania z ryzykiem.
 - 5) Opracowanie/aktualizacja procedury bezpieczeństwa fizycznego obejmująca obowiązek wyznaczenia osoby odpowiedzialnej za bezpieczeństwo fizyczne,
 - 6) Opracowanie/aktualizacja zasad odpowiedzialności za cyberbezpieczeństwo wraz ze wskazaniem obowiązku wyznaczenia osoby odpowiedzialnej za cyberbezpieczeństwo,
 - 7) Opracowanie/aktualizacja treści zarządzenia wdrażającego SZBI dla Zamawiającego,
 - 8) Opracowanie/aktualizacja planu postępowania z ryzykiem obejmującym systematyczne tworzenie raportów oceny ryzyka oraz konieczność cyklicznego przeglądu tego raportu,
 - 9) Opracowanie/aktualizacja szczegółowego sposobu realizacji celów oraz we współpracy z Zamawiającym przypisanie odpowiedzialności za ich realizację,

- 10) Opracowanie/aktualizacja procedury wprowadzającej obowiązek regularnego, corocznego przeglądu Polityki Bezpieczeństwa Informacji (PBI),
 - 11) Opracowanie/aktualizacja polityki szkoleń obejmującej obowiązek informowania o zmianach w PBI w toku okresowych szkoleń stanowiskowych,
 - 12) Opracowanie/aktualizacja procedur zarządzania aktywami informacyjnymi,
 - 13) Opracowanie/aktualizacja procedur oceny ryzyka z uwzględnieniem aktywów informacyjnych,
 - 14) Opracowanie/aktualizacja zagrożeń związanych z cyberbezpieczeństwem w ramach procesów zarządczych oraz zarządzania ryzykiem,
 - 15) Opracowanie/aktualizacja planu postępowania z ryzykiem związanym z zagrożeniami bezpieczeństwa informacji,
 - 16) Opracowanie/aktualizacja kompleksowej polityki zarządzania ryzykiem,
 - 17) Opracowanie/aktualizacja kompleksowej polityki zarządzania ryzykiem uwzględniającej obowiązek identyfikacji i priorytetyzacji odpowiedzi na ryzyka,
 - 18) Opracowanie/aktualizacja kompleksowej polityki zarządzania ryzykiem uwzględniającej system oceny ryzyka,
 - 19) Opracowanie/aktualizacja kompleksowej polityki zarządzania ryzykiem cyberbezpieczeństwa uwzględniającej identyfikowanie, ustanawianie i ocenianie ryzyka,
 - 20) Opracowanie/aktualizacja kompleksowej polityki zarządzania danymi uwzględniającej politykę ich niszczenia, plan backup, plany reagowania i odtwarzania danych,
 - 21) Opracowanie/aktualizacja planu zarządzania podatnościami,
 - 22) Opracowanie/aktualizacja kompleksowej polityki zarządzania zapisami zdarzeń, logów, inspekcji,
 - 23) Opracowanie/aktualizacja polityki użytkowania dostępu do odczytu lub zapisu danych z zewnętrznych nośników danych,
 - 24) Opracowanie/aktualizacja kompleksowej polityki reagowania na incydenty uwzględniającej procedury procesowania incydentów,
 - 25) Opracowanie/aktualizacja planu zarządzania podatnościami uwzględniającego obowiązek dokumentowania ryzyka z nim związanego,
 - 26) Opracowanie/aktualizacja polityki reagowania na incydenty uwzględniającej procedurę procesowania incydentów i ich aktualizacji w obszarze doświadczeń i wniosków z wykrytych i obsłużonych incydentów,
 - 27) Opracowanie/aktualizacja polityki reagowania na incydenty uwzględniającej procedurę procesowania incydentów wraz z obowiązkiem ich aktualizacji,
 - 28) Opracowanie/aktualizacja polityki planów odtwarzania uwzględniającej obowiązek ich aktualizacji w obszarze doświadczeń i wniosków z prowadzonych procesów odtwarzania.
- Wykonawca będzie realizował usługę według następujących etapów:
- a) Etap 1 – Audyt zerowy – sprawdzenie spełnienia wymagań zaleceń w ramach standardów PN-EN ISO/IEC 27001:2023 i norm pokrewnych,
 - b) Etap 2 – Zastosowanie zabezpieczeń na podstawie zaleceń po audytowych:
 - konsultacje przy wdrożeniu zabezpieczeń w infrastrukturze systemu informatycznego,
 - konsultacje przy wdrożeniu zabezpieczeń organizacyjnych – polityki bezpieczeństwa danych osobowych, zapisów w umowach z dostawcami itp.,
 - c) Etap 3 – Planowanie SZBI:
 - przeprowadzenie instruktażu dla kadry zarządzającej z zasad bezpieczeństwa informacji,
 - zdefiniowanie wymaganych polityk SZBI,
 - wybór celów zabezpieczeń,
 - d) Etap 4 – Inwentaryzacja i szacowanie ryzyka SZBI:
 - przeprowadzenie instruktaży dla pracowników oraz kadry zarządzającej z metody inwentaryzacji i klasyfikacji aktywów informacyjnych,

- wykonanie wraz z pracownikami inwentaryzacji i klasyfikacji aktywów informacyjnych,
 - zdefiniowanie planu postępowania z ryzykiem,
 - opracowanie raportu z oceny ryzyka,
- e) Etap 5 – Opracowanie niezbędnej dokumentacji SZBI:
- opracowanie wspólne z pracownikami Zamawiającego wymaganych procedur i instrukcji,
 - wykonanie projektu zabezpieczeń – opracowanie projektu zabezpieczeń i konsultacje przy wdrożeniu odpowiednio skutecznych zabezpieczeń zgodnych z celami zabezpieczeń.
 - opracowanie programu uświadamiania i szkolenia,
 - przeprowadzenie instruktaży dla pracowników z dokumentacji ochrony informacji,
 - przeprowadzenie instruktaży dla kadry zarządzającej z dokumentacji ochrony informacji,
- f) Etap 6 – Weryfikacja i monitorowanie SZBI:
- przeprowadzenie wraz z pracownikami organizacji audytu wewnętrznego,
 - opracowanie raportu z audytu wewnętrznego,
4. Wykonawca zapewni w ramach realizowanych usług dostęp do oprogramowania wspomagającego zarządzanie i realizację audytów wewnętrznych przez okres 12 miesięcy od dnia przekazania Zamawiającemu zaktualizowanej dokumentacji SZBI. Oprogramowanie udostępnione przez Wykonawcę powinno spełniać następujące wymagania:
- 1) System powinien zawierać moduł konfiguracji pozwalający na:
 - a) zarządzanie użytkownikami,
 - b) zarządzanie uprawnieniami użytkowników,
 - c) definicję struktury organizacyjnej,
 - d) generowanie kodów QR dla obszarów audytowych,
 - e) definicję list audytowych, składających się z jednej lub kilku grup pytań (łączenie różnych typów): różne typy pytań (otwarte, liczbowe, punktowe, z/bez zdjęcia, z/bez niezgodności), możliwość definicji dostępnych odpowiedzi (tekst, waga, kolorystyka), możliwość przypisania list do audytów i obszarów audytowych,
 - f) konfigurację wysyłki raportów audytowych,
 - g) konfigurację rejestrów dodatkowych (zarządzanie uprawnieniami: dostępu, rozwiązywania, powiadomienia mailowe, możliwość definicji pól dodatkowych, przypisanie struktury),
 - h) konfigurację nieograniczonej ilości list audytowych, rejestrów i obszarów,
 - i) konfigurację nieograniczonej ilości wykonywania audytów i zgłoszeń,
 - j) brak zapisu danych (w tym wykonywanych zdjęć) na urządzeniu obsługującym system.
 - 2) System powinien zawierać moduł harmonogramowania audytów pozwalający na:
 - a) możliwość planowania audytów dla obszarów i audytorów,
 - b) możliwość planowania dla grup obszarów (ścieżek) i grup audytorów,
 - c) obsługa harmonogramów miesięcznych i tygodniowych,
 - d) możliwość zaplanowania audytów na konkretny dzień,
 - e) możliwość zaplanowania audytów na cały okres (tydzień, miesiąc),
 - f) powiadomienia mailowe (informacja o zaplanowaniu audytu, przypomnienie o zbliżającym się terminie realizacji),
 - g) możliwość automatycznego generowania harmonogramu zgodnie z zadanymi kryteriami (wybór obszarów, audytorów, częstotliwości audytów),
 - h) możliwość kopiowania stworzonych harmonogramów.
 - 3) System powinien zawierać moduł wykonywania audytów pozwalający na:
 - a) możliwość wykonywania audytów na urządzeniach mobilnych (Android),
 - b) możliwość realizacji kilku audytów równolegle przez jednego użytkownika (w obrębie tej samej listy audytowej i różnych list),

- c) możliwość równoległej realizacji przez kilku użytkowników tej samej listy audytowej,
 - d) możliwość przerwania audytu w trakcie i jego wznowienie bez utraty danych,
 - e) możliwość skanowania kodów QR obszarów audytowych,
 - f) możliwość wskazania audytowanego wyrobu (dla list audytowych dotyczących audytu wyrobu),
 - g) możliwość skanowania kodów QR wyrobu,
 - h) możliwość dodawania zdjęć i opisów,
 - i) możliwość pominięcia pytania lub całej grupy pytań (obniżenie maksymalnej ilości punktów jaka była możliwa do otrzymania),
 - j) możliwość realizacji audytów z/bez harmonogramu (lub tylko z harmonogramu),
 - k) możliwość realizacji ścieżek audytowych (zdefiniowanej grupy obszarów),
 - l) automatyczne generowanie raportów z audytów w formacie pdf i wysyłka mailowa zgodna z konfiguracją do właściwych osób.
- 4) System powinien zawierać moduł zarządzania niezgodnościami i działaniami pozwalającymi na:
- a) automatyczne rejestrowanie niezgodności audytowych do rejestrów,
 - b) możliwość przeglądu i rozwiązywania zgłoszeń (uprawnione osoby, zgodnie ze strukturą organizacyjną),
 - c) możliwość tworzenia planów działań (dla każdego działania możliwość określenia osoby realizującej, terminu realizacji, opisu),
 - d) obsługa zdjęć i załączników (w formatach biurowych),
 - e) powiadomienia mailowe (zaplanowanie działania, modyfikacja, zbliżający się termin realizacji).
- 5) System powinien zawierać moduł zarządzania rejestrami pozwalającymi na:
- a) możliwość rejestracji zgłoszeń nieaudytowych (ad hoc) przez uprawnionych użytkowników,
 - b) możliwość dodawania zdjęć i załączników,
 - c) obsługę konfigurowalnych powiadomień mailowych,
 - d) możliwość rejestracji zgłoszenia bez posiadania konta użytkownika.
- 6) System powinien zawierać moduł statystyk pozwalający na:
- a) statystyki wyników audytowych (wg struktury),
 - b) statystyki niezgodności (wg osoby zgłaszającej, osoby odpowiedzialnej, obszaru),
 - c) statystyki działań (wg osoby planującej, osoby realizującej, obszaru),
 - d) statystyki realizacji harmonogramu (wg audytora, obszaru).