

Załącznik – Wymagania dotyczące Bezpieczeństwa Informacji i Cyberbezpieczeństwo dla Wykonawcy.

1. Wymagania organizacyjne:

- a) Wykonawca zobowiązuje się do zapoznania z wdrożonymi i stosowanymi w organizacji politykami bezpieczeństwa informacji.
- b) Wykonawca zobowiązuje się do przedstawienia swoich wdrożonych i stosowanych w organizacji polityk bezpieczeństwa informacji.
- c) Polityki i procedury bezpieczeństwa informacji wdrożone oraz stosowane w obu organizacjach muszą być zgodne ze standardami rodziny normy ISO 27001 i IEC 62443.
- d) Wykonawca zapewnia, że wszyscy pracownicy i podwykonawcy biorący udział w projekcie mają podpisane zobowiązania do zachowania poufności w postaci umowy NDA.
- e) Wykonawca i Zleceniodawca prowadzą rejestr osób mających dostęp do danych i systemu. Rejestr musi być udostępniany między stronami w celu weryfikacji, a udostępnione dane monitorowane pod względem zachowania poufności, integralności i dostępności.

2. Wymagania dotyczące ochrony danych i zachowania zasad poufności:

- a) Dane przetwarzane w systemach związanych z projektem Zleceniodawcy i Wykonawcy muszą być chronione zgodnie z zasadą zachowania poufności, integralności i dostępności. Jeżeli dane są udostępniane poza organizację obu podmiotów, zasady bezpieczeństwa informacji muszą zostać zachowane przez wszystkie strony umowy na podstawie standardów ISO 27001.
- b) Wszelkie dane wrażliwe, poufne, niejawne i tajne muszą być zabezpieczane według zatwierdzonych procedur i narzędzi. Dokumenty posiadające informacje i dane oznaczone jako wrażliwe muszą być zabezpieczone protokołem szyfrowania lub hasłem.
- c) Wykonawca nie może wykorzystywać danych do celów innych niż określonych w umowie z Zleceniodawcą.

3. Wymagania dotyczące architektury i bezpieczeństwa technicznego:

- a) Infrastruktura musi być zaprojektowana zgodnie ze standardami rodziny norm ISO i IEC, stosując jednocześnie zasady „security by design” oraz „privacy by design”.
- b) Infrastruktura musi być zaprojektowana w taki sposób, aby umożliwić wdrożenie dodatkowych mechanizmów, w tym zewnętrznej kontroli dostępu i monitorowania infrastruktury.

- c) Wykonawca zapewnia wdrożenie narzędzi do zbierania informacji i zdarzeń bezpieczeństwa oraz ich ochronę przed modyfikacją w trakcie trwania projektu.
- d) Przeprowadzanie przez Wykonawcę regularnych testów podatności w infrastrukturze i jej elementów. Przekazywanie pozyskanych z nich informacji Zleceniodawcy.

4. Wymagania dotyczące infrastruktury:

- a) Wykonawca zapewnia aktualizację urządzeń, systemów operacyjnych, programów, baz danych i komponentów w trakcie trwania projektu.
- b) Wykonawca zapewnia instalację i wdrożenie zabezpieczeń sieciowych, do których zaliczamy urządzenia zapory sieciowej – UTM, konfigurację przełączników oraz zastosowanie segmentacji sieci.
- c) Wykonawca zapewnia regularne testy podatności zarządzanymi urządzeniami i systemami w infrastrukturze.

5. Wymagania dotyczące zarządzania tożsamością i polityką dostępu:

- a) Wykonawca jest zobowiązany do stosowania narzędzi zabezpieczających, takich jak wieloskładnikowe (MFA) lub dwuskładnikowe (2FA).
- b) Stosowanie silnych haseł zgodnych z polityką bezpieczeństwa i polityką haseł.
- c) Zarządzanie dostępem wyłącznie dla osób potwierdzonych i wyznaczonych przez organizację.
- d) Wykonywanie regularnych przeglądów uprawnień użytkowników i logów wejść użytkowników.

6. Wymagania dotyczące ciągłości działania i kopii zapasowych:

- a) Wykonawca ma obowiązek przygotowania planu ciągłości działania i plan odtwarzania po awarii.
- b) Kopie zapasowe muszą być wykonywane regularnie, według zatwierdzonych ustaleń z Wykonawcą. Kopia zapasowa musi być przechowywana w bezpiecznej lokalizacji, zatwierdzonej przez Zleceniodawcę.
- c) Testy odtwarzania danych muszą być przeprowadzane co najmniej raz w roku, na podstawie zatwierdzonych procedur bezpieczeństwa informacji.

7. Wymagania dotyczące monitorowania infrastruktury i audytu:

- a) Monitorowanie sieci musi odbywać się jako proces nieprzerwany, stosując zasadę 24/7/365.
- b) Logi muszą być przechowywane przez okres określony i lokalizacji w umowie.

- c) Wykonawca umożliwi przeprowadzenie audytu bezpieczeństwa przez Zamawiającego.
- d) Wykonawca zobowiązuje się do niezwłocznego zgłaszania incydentów bezpieczeństwa ustalonych z Zleceniodawcą.

8. Wymagania dotyczące incydentów bezpieczeństwa:

- a) Wykonawca musi posiadać procedurę zarządzania i reagowania na incydenty.
- b) W przypadku naruszenia danych osobowych Wykonawca musi zgłosić incydent do Zleceniodawcy oraz odpowiednich w.
- c) Wykonawca zapewnia wykonanie analizy incydentu i wdrożenie działań naprawczych po zakończeniu procesu analizy.

9. Wymagania dotyczące dokumentacji:

- a) Wykonawca dostarcza pełną dokumentację bezpieczeństwa, do których zaliczamy:
 - o Politykę bezpieczeństwa informacji,
 - o Politykę Zarządzania Systemem,
 - o Procedurę tworzenia kopii zapasowych i odtwarzania,
 - o Procedurę nadawania i odbierania uprawnień,
 - o Zarządzanie i rejestr incydentów.
 - o Inne, wymagane przez regulacje prawne i przepisy.
- b) Dokumentacja musi być aktualizowana przed zakończeniem projektu.

10. Wymagania dotyczące podwykonawców:

- a) Wykonawca ponosi pełną odpowiedzialność za działania podwykonawców w trakcie .
- b) Podwykonawcy muszą spełniać te same wymagania bezpieczeństwa co Wykonawca.
- c) Wykonawca musi uzyskać zgodę Zamawiającego na korzystanie z podwykonawców.