**Załącznik nr 1 do Umowy nr …… z dnia ……………**

**Opis przedmiotu zamówienia**

1. **Zakres przedmiotu zamówienia:**

*Aktualizacja lub wprowadzenie Polityki Bezpieczeństwa Informacji (PBI) w:*

1. Starostwie Powiatowym w Głogowie
2. I Liceum Ogólnokształcącym im. Bolesława Krzywoustego w Głogowe
3. II Liceum Ogólnokształcącym im. Mikołaja Kopernika w Głogowie
4. Zespole Szkół Technicznych i Ogólnokształcących w Głogowie
5. Zespole Szkół Ekonomicznych im. Jana Pawła II w Głogowie
6. Zespole Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie
7. Zespole Szkół Przyrodniczych i Branżowych w Głogowie
8. Zespole Szkół Politechnicznych w Głogowie
9. Zespole Szkół im. Jana Wyżykowskiego w Głogowie
10. Zespole Placówek Szkolno – Wychowawczych w Głogowie
11. Powiatowym Centrum Poradnictwa Psychologiczno – Pedagogicznego i Doskonalenia Nauczycieli w Głogowie
12. Głogowskim Centrum Kształcenia Zawodowej w Głogowie
13. Powiatowym Centrum Pomocy Rodzinie w Głogowie
14. Domu Pomocy Społecznej „Magnolia” w Głogowie
15. Powiatowym Środowiskowym Domu Samopomocy w Głogowie
16. Powiatowym Centrum Administracyjnym w Głogowie
17. Powiatowym Urzędzie Pracy w Głogowie
18. Powiatowym Ośrodku Dokumentacji Geodezyjnej i Kartograficznej w Głogowie

spełniającej wymagania norm rodziny ISO 27000 w zakresie bezpieczeństwa informacji
(w szczególności zgodnego z wymaganiami aktualnych norm PN-EN ISO/IEC 27001 oraz zaleceniami aktualnych norm PN-ISO/IEC 27002, PN-ISO-27005) i ISO 31000 w zakresie zarządzania ryzykiem oraz Systemu Zarządzania Ciągłością Działania – w zakresie systemów teleinformatycznych zgodnego z normą PN-EN ISO 22301.

Wykonawca zobowiązany jest wytworzyć spójne, jednolite, adekwatne do faktycznych ryzyk, procesów i potrzeb dokumentacje SZBI zgodne z wymaganiami powołanych wyżej norm w celu spełnienia wymagań wynikających z:

* rozporządzenia Rady Ministrów z dnia 21.05.2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
* ustawy z dnia z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa;
* rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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),
* dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (NIS2).
1. **Ogólny zakres zadań Wykonawcy:**
2. Wykonanie audytu wstępnego obejmującego min.:
* inwentaryzację uprawnień w programach i systemach informatycznych,
* inwentaryzację aktywów,
* rozpoznanie struktury organizacyjnej i realizowanych procesów oraz wymagań prawnych funkcjonowania jednostki.
1. Stworzenie dokumentacji SZBI z uwzględnieniem istniejących procedur.
2. Opracowanie zasad i formularzy dotyczących nadawania i odbierania uprawnień
 w programach informatycznych.
3. Analiza całościowa PBI, dokumentacji Ochrony Danych Osobowych i dokumentacji Bezpieczeństwa Systemów Informatycznych, weryfikacja powiązań i zależności oraz ocena pod kątem zgodności z wymogami norm i przepisów powołanych na wstępie.
4. Pomoc przy inwentaryzacji aktywów oraz przypisaniu własności aktywów.
5. Analiza ryzyka i opracowanie planu postępowania z ryzykiem.
6. Dostosowanie procedur do istniejącego ryzyka.
7. Opracowanie planu ciągłości działania.
8. Pełnienie po trzy dyżury w każdej jednostce objętej zamówieniem w czasie trwania umowy, przy czym każdy dyżur winien trwać po 2 godziny i obejmować przeszkolenie wskazanych osób z kadry kierowniczej oraz konsultacje z przedstawicielem Zamawiającego.

Przeszkolenie kadry kierowniczej 18 jednostek objętych przedmiotem zamówienia obejmuje zakresu funkcjonowania i stosowania SZBI.

1. Pomoc przy wykonaniu analizy ryzyka.
2. Opracowanie działań korygujących i zapobiegawczych.
3. Przygotowanie harmonogramu przeglądów funkcjonowania SZBI.
4. **Wymagania dotyczące Polityki Bezpieczeństwa Informacji:**

Zamawiający wymaga aby wdrożona Polityka Bezpieczeństwa Informacji w sposób usystematyzowany oraz jednoznaczny opisywała i regulowała wymienione niżej zagadnienia oraz obszary funkcjonowania wynikające bezpośrednio z celów stosowania zabezpieczeń stanowiących załącznik A do normy ISO/IEC 27001.

Polityka Bezpieczeństwa Informacji (zagadnienia ogólne):

* znaczenie bezpieczeństwa informacji dla organizacji
* cele jakie organizacja zamierza osiągnąć w zakresie bezpieczeństwa informacji,
* obszar stosowania polityki,
* zgodność z obowiązującymi przepisami i normami.

Organizacja bezpieczeństwa informacji:

* role i odpowiedzialność za bezpieczeństwo informacji,
* rozdzielanie obowiązków,
* bezpieczeństwo informacji w zarządzaniu projektami,
* polityka stosowania urządzeń mobilnych,
* telepraca.

Bezpieczeństwo zasobów ludzkich:

* postępowanie sprawdzające przed zatrudnieniem,
* warunki zatrudnienia,
* odpowiedzialność kierownictwa,
* uświadamianie i szkolenia z zakresu bezpieczeństwa informacji
* zakończenie zatrudnienia i zmiana zakresu obowiązków.

Zarządzanie aktywami:

* inwentaryzacja aktywów,
* własność aktywów,
* akceptowalne użycie aktywów,
* zwrot aktywów,
* klasyfikowanie informacji
* oznaczanie informacji
* postępowanie z aktywami,
* zarządzanie nośnikami wymiennymi,
* wycofywanie nośników,
* przekazywanie nośników.

Kontrola dostępu:

* polityka kontroli dostępu,
* dostęp do sieci i usług sieciowych,
* rejestrowanie i wyrejestrowanie użytkowników,
* przydzielanie dostępu użytkownikom,
* zarządzanie prawami uprzywilejowanego dostępu (w tym zasady funkcjonowania administratorów podstawowych, takich jak np.: admin, administrator, root),
* przegląd praw dostępu użytkowników,
* odbieranie lub dostosowanie praw dostępu,
* stosowanie poufnych informacji uwierzytelniających,
* ograniczanie dostępu do informacji.
* procedury bezpiecznego logowania,
* system zarządzania hasłami,
* użycie uprzywilejowanych programów narzędziowych,
* kontrola dostępu do kodów źródłowych programów,

Kryptografia:

* polityka stosowania zabezpieczeń kryptograficznych,
* zarządzanie kluczami.

Bezpieczeństwo fizyczne i środowiskowe.

* fizyczna granica obszaru bezpiecznego,
* fizyczne zabezpieczenie wejść,
* zabezpieczenie biur, pomieszczeń i obiektów,
* ochrona przed zagrożeniami zewnętrznymi i środowiskowymi,
* praca w obszarach bezpiecznych,
* obszary dostaw i załadunku,
* lokalizacja i ochrona sprzętu,
* systemy wspomagające,
* bezpieczeństwo okablowania,
* konserwacja sprzętu,
* wynoszenie aktywów,
* bezpieczeństwo sprzętu i aktywów poza siedzibą,
* bezpieczne zbywanie lub przekazywanie do ponownego użycia
* pozostawienie sprzętu użytkownika bez opieki,
* polityka czystego biurka i czystego ekranu.

Bezpieczna eksploatacja:

* dokumentowanie procedur eksploatacyjnych,
* zarządzanie zmianami,
* zarządzanie pojemnością,
* zabezpieczenia przed szkodliwym oprogramowaniem,
* kopie zapasowe,
* rejestrowanie zdarzeń,
* ochrona informacji w dziennikach zdarzeń,
* rejestrowanie działań administratorów i operatorów,
* synchronizacja zegarów,
* instalacja oprogramowania w systemach produkcyjnych,
* zarządzanie podatnościami technicznymi,
* ograniczenia w instalowaniu oprogramowania.

Bezpieczeństwo komunikacji:

* zabezpieczenia sieci,
* bezpieczeństwo usług sieciowych,
* rozdzielanie sieci,
* polityki i procedury przesyłania informacji,
* wiadomości elektroniczne.

Pozyskiwanie, rozwój i utrzymanie systemów:

* analiza i specyfikacja wymagań bezpieczeństwa informacji,
* zabezpieczanie usług aplikacyjnych w sieciach publicznych,
* procedury kontroli zmian w systemach.

Analiza ryzyka:

* zasady przeprowadzania,
* sposób oceny ryzyk,
* zasady zarządzania ryzykiem,

Plan ciągłości działania:

* identyfikacja kluczowych zasobów, procesów, usług i dostawców,
* scenariusze utraty ciągłości działania,
* zasady komunikacji w sytuacjach kryzysowych,
* plany przywracania ciągłości działania,
* redundancja zasobów i usług kluczowych,
* zasady testowania planu.
1. **Wymagania dotyczące bezpieczeństwa systemu informatycznego**

Zamawiający wymaga aby wszystkie zagadnienia odnoszące się bezpośrednio do systemu informatycznego opracowane były w wydzielonym dokumencie do zapisów którego odnosić się będą zarówno Polityka Bezpieczeństwa Informacji oraz dokument opisujący zasady ochrony danych osobowych. Zamawiający wymaga aby dokument ten regulował następujący zakres działań/zagadnień:

* nadawanie uprawnień użytkownikom systemów informatycznych należących do Zamawiającego w sposób precyzyjny i jednoznaczny ,
* zasady nadawania uprawnień uprzywilejowanych (ASI),
* nadawanie uprawnień w systemach informatycznych niepodlegających nadzorowi ze strony administratora lokalnego (np. ZUS PUE, GUS, ePUAP),
* organizacja certyfikatów SSL,
* organizacja kluczy szyfrujących,
* zasady użytkowania zewnętrznych nośników informacji,
* zasady użytkowania komputerów mobilnych,
* zasady wykonywania pracy zdalnej przez pracowników Zamawiającego,
* zasady nawiązywania połączeń zdalnych przez wsparcie techniczne producentów programów (w trybie nadzorowanym i nienadzorowanym),
* zasady nawiązywania połączeń zdalnych przez Administratorów Systemu Informatycznego,
* archiwizacja danych i testowanie kopii bezpieczeństwa,
* kontrola dostępu do sieci, systemu i aplikacji
* użytkowanie i zabezpieczenia stanowiska użytkownika
* bezpieczeństwo fizyczne i środowiskowe
* kontrola połączeń z siecią publiczną
* zasady wykorzystania zabezpieczeń kryptograficznych
* aktualizacja oprogramowania

Dokumentacja opisująca zasady funkcjonowania i kontroli systemu informatycznego powinna zawierać szablony wszystkich wykazów i rejestrów które powinny być prowadzone przez użytkowników lub administratorów systemu informatycznego.

**V Ochrona danych osobowych**

Przedmiotem zamówienia nie jest wdrożenie dokumentów wynikających z RODO, np. PODO. Jednostki posiadają dokumentacje dotyczącą ochrony danych osobowych.