**Zamawiający:**

**Powiat Białobrzeski**

**Plac Zygmunta Starego 9**

**26-800 Białobrzegi**

**NIP: 798 14 64 078, REGON: 670223132**

**Załącznik nr 1– Opis przedmiotu zamówienia**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Przedmiotem zamówienia jest opracowanie dokumentacji z zakresu Systemu Zarządzania Bezpieczeństwem Informacji** w oparciu o normę ISO IEC 27001 dla Powiatu Białobrzeskiego w ramach Projektu Grantowego pn. „Cyberbezpieczny Samorząd” realizowany jest w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa”.

Zamawiający wymaga wykonania usługi zgodnie z wymaganiami bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych oraz aktualnie obowiązującymi normami PN-EN ISO 27001 oraz PN-EN ISO 22301, w ramach Projektu Grantowego pn. „Cyberbezpieczny Samorząd” realizowanego
w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa”.

**Wymagane, aby opracowana dokumentacja spełniała poniższe wymagania minimalne:**

**I. Cel i przedmiot zamówienia**:

Wdrożenie ma na celu zwiększenie poziomu ochrony informacji oraz zapewnienie ciągłości działania w jednostce poprzez **kompleksowe opracowanie, wdrożenie, przegląd i aktualizację dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)**. Rezultat ma być w pełni zgodny z wymogami krajowymi (w tym ustawy o krajowym systemie cyberbezpieczeństwa – uoKSC, Krajowych Ram Interoperacyjności – KRI) oraz z uznanymi standardami międzynarodowymi (ISO 27001, ISO 22301)

1. **Przedmiot zamówienia:**
Przedmiotem jest opracowanie i wdrożenie **kompletu dokumentów** (polityk, procedur, planów i instrukcji) obejmujących obszary:
	1. Polityka Bezpieczeństwa Informacji (PBI),
	2. Polityka Bezpieczeństwa Fizycznego,
	3. Polityka Bezpieczeństwa Teleinformatycznego,
	4. Polityka Ciągłości Działania.

Dodatkowo Wykonawca zobowiązany jest do przeprowadzenia niezbędnych testów, pozwalających ocenić skuteczność wdrożonych rozwiązań.

**II. Zakres i ogólne wymagania**

1. **Opracowanie i aktualizacja dokumentacji**
Wykonawca przygotuje szczegółowe dokumenty i zaktualizuje istniejące, regulujące procesy związane z bezpieczeństwem informacji. Muszą one uwzględniać m.in. procedury obsługi incydentów, zasady kontroli dostępu, zarządzanie ryzykiem, bezpieczeństwo pracy zdalnej, wykorzystanie urządzeń mobilnych, szyfrowanie danych, a także planowanie i utrzymanie ciągłości działania.
2. **Wdrożenie i praktyczne zastosowanie**
Opracowane dokumenty mają być wdrożone w taki sposób, aby pracownicy, współpracownicy i dostawcy rozumieli i stosowali określone zasady. W ramach wdrożenia należy uwzględnić:
	1. Instrukcje postępowania (operacyjne) i materiały informacyjne,
	2. Narzędzia wspierające (rejestry incydentów, wzory formularzy).
3. **Przegląd, testowanie i aktualizacja**
Po wdrożeniu dokumentacji konieczne jest zaplanowanie i wykonanie przeglądów oraz testów (np. symulacje incydentów, testy planów ciągłości działania), dzięki którym będzie można wykryć ewentualne niezgodności, niedostatki i wprowadzić działania korygujące.
4. **Zgodność z przepisami i normami**
Dokumentacja musi uwzględniać aktualne przepisy (w tym RODO, ustawę o ochronie danych osobowych, ustawę o krajowym systemie cyberbezpieczeństwa) oraz wytyczne dedykowane administracji publicznej (KRI). Ponadto powinna być spójna z normami ISO 27001 (w zakresie bezpieczeństwa informacji) oraz ISO 22301 (w zakresie ciągłości działania).
5. **Pełna integracja w ramach SZBI**
Wymagane jest, aby wszystkie opracowane polityki i procedury stanowiły część jednego, spójnego Systemu Zarządzania Bezpieczeństwem Informacji. System ten ma zapewniać skuteczne zarządzanie ryzykiem, reagowanie na incydenty, ochronę fizyczną i teleinformatyczną, a także nieprzerwane działanie kluczowych procesów jednostki.

**III. Szczegółowy opis zadań Wykonawcy**

Wykonawca zobowiązany jest do realizacji następujących zadań:

**3.1. Analiza stanu obecnego i przygotowanie koncepcji**

* Przegląd obecnych procedur, regulacji i narzędzi.
* Ocena zgodności z wymogami prawnymi (KRI, uoKSC, RODO) oraz z celami jednostki.
* Określenie zakresu i harmonogramu prac wdrożeniowych.

**3.2. Opracowanie / aktualizacja dokumentacji SZBI**

* Sporządzenie kompletu dokumentów, opisanych w tabeli (rozdział 4), z uwzględnieniem specyfiki jednostki.
* Ujednolicenie struktury polityk, procedur i instrukcji, tak aby stanowiły spójny system.
* Przygotowanie materiałów pomocniczych (np. formularzy, rejestrów, checklist).

**3.3. Wdrożenie**

* Zaplanowanie szkoleń zwiększających świadomość i umiejętności pracowników w obszarze bezpieczeństwa informacji.
* Włączenie opracowanych procedur w codzienne funkcjonowanie urzędu (konfiguracja systemów, zmiany w organizacji pracy).
* Udostępnienie wzorów raportów, ewidencji i innych dokumentów operacyjnych.

**3.4. Testy, przegląd i aktualizacja**

W celu zapewnienia weryfikacji wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) należy przeprowadzić specjalistyczne testy bezpieczeństwa z udziałem Zamawiającego. Wykonawca niniejszego zamówienia przeprowadza testy wdrożonego SZBI oraz wspiera Zamawiającego w analizie raportu końcowego i wdrożeniu rekomendacji poaudytowych – w szczególności poprzez aktualizację dokumentacji SZBI, zaplanowanie działań korygujących i zapobiegawczych w obszarach wskazanych w raporcie oraz przeprowadzenie ponownych testów wybranych elementów, jeśli będzie to konieczne dla potwierdzenia usunięcia zidentyfikowanych podatności.

**3.5. Opracowanie raportu końcowego i przekazanie dokumentacji**

* Sporządzenie końcowego raportu z wykonanych prac, wniosków i rekomendacji.
* Przekazanie dokumentacji (w formie elektronicznej i – na życzenie Zamawiającego – papierowej) wraz z prawami autorskimi majątkowymi.
* Udokumentowanie wdrożenia w postaci protokołu odbioru.

**IV. Wymagane dokumenty i ich zakres – zestawienie tabelaryczne**

W poniższej tabeli zaprezentowano **kompletny wykaz** polityk i procedur, jakie mają zostać opracowane, wdrożone lub zaktualizowane w ramach SZBI.

**4.1. Polityka Bezpieczeństwa Informacji (PBI)**

|  |  |
| --- | --- |
| Dokument | Opis / Zakres |
| Procedura czystego biurka i czystego ekranu | Zasady utrzymywania porządku na stanowiskach pracy, tak aby poufne dane (zarówno w formie papierowej, jak i elektronicznej) nie były narażone na wgląd osób nieuprawnionych.  |
| Procedura klasyfikacji informacji | Dokument definiujący kategorie ochrony informacji (np. jawne, poufne, wrażliwe), kryteria ich przydzielania oraz sposoby znakowania i przechowywania. Celem jest jasne określenie, jakie poziomy ochrony stosuje się do różnego typu danych, co pozwala zapobiegać niekontrolowanemu ujawnieniu treści o istotnym znaczeniu. |
| Procedura bezpieczeństwa zasobów ludzkich | Wytyczne w zakresie rekrutacji, szkolenia i wyrejestrowywania pracowników z systemów IT. Uregulowanie zasad podpisywania oświadczeń o zachowaniu poufności, monitoringu przestrzegania polityk bezpieczeństwa przez personel, a także tryb postępowania w przypadku naruszeń lub odejścia pracownika. |
| Procedura zarządzania relacjami z dostawcami | Obejmuje cały cykl zarządzania podmiotami zewnętrznymi, które otrzymują dostęp do informacji bądź systemów urzędu (np. dostawcy usług IT). Dokument określający m.in. zasady umów powierzenia, ocenę bezpieczeństwa dostawcy, audyty zgodności, mechanizmy weryfikacji. |
| Plan szkoleń i podnoszenia świadomości | Szczegółowe omówienie sposobów i częstotliwości prowadzenia szkoleń dotyczących ochrony informacji.  |
| Procedura przeprowadzania audytów wewnętrznych | Zasady cyklicznych kontroli wewnętrznych oceniających zgodność z politykami bezpieczeństwa, przepisami (KRI, uoKSC) i normami (ISO 27001). Procedura ta określająca zakres, harmonogram, odpowiedzialność, sposób raportowania i analizowania wyników audytów w celu wykrycia ewentualnych niezgodności. |
| Procedura działań doskonalących | Definiuje proces ciągłego doskonalenia SZBI. Po zidentyfikowaniu problemów wyjaśnia, jak zaplanować, przeprowadzić i weryfikować skuteczność działań korygujących i zapobiegawczych.  |
| Procedura kontroli dokumentów i zapisów | Regulacja określająca cykl życia dokumentacji: tworzenie, weryfikację, autoryzację, wprowadzanie zmian, archiwizację i niszczenie. Zawiera zasady nadawania numerów wersji, prowadzenia rejestrów dokumentów oraz monitorowania ważności procedur. |
| Metodologia szacowania ryzyka | Wskazuje sposób identyfikacji zagrożeń, oceny prawdopodobieństwa i skutków ewentualnych incydentów, a także określania priorytetów w zarządzaniu ryzykiem. Powinna opierać się na uznanych praktykach (np. ISO 27001) i być kompatybilna z wymaganiami KRI/uoKSC. |

**4.2. Polityka Bezpieczeństwa Fizycznego**

|  |  |
| --- | --- |
| Dokument | Opis / Zakres |
| Wzór ewidencji dostępu do pomieszczeń | Określa format i sposób prowadzenia rejestru wejść i wyjść z obszarów o ograniczonym dostępie. Pomaga monitorować i kontrolować ruch osobowy, minimalizując ryzyko nieautoryzowanego wejścia do stref chronionych (np. serwerownia, archiwum). |
| Polityka kluczy | Zbiór zasad przydzielania, przechowywania i zwrotu kluczy (bądź kart dostępu) do pomieszczeń chronionych. Definiuje środki zapobiegawcze (ewidencja, okresowa inwentaryzacja) i postępowanie w przypadku zagubienia/kradzieży kluczy. |
| Wykaz pomieszczeń tworzących obszar przetwarzania danych | Lista pomieszczeń (lub stref) w których dochodzi do przetwarzania danych szczególnie chronionych. Określa kategorie dostępu i wymagane zabezpieczenia. |
| Procedura dotycząca pracy w zabezpieczonych obszarach | Instrukcja postępowania dla personelu i osób zewnętrznych przebywających w obszarach o podwyższonym poziomie ochrony. Zawiera m.in. zasady weryfikacji tożsamości, konieczność rejestracji wizyt, dozwolone/zakazane działania (np. fotografowanie, nagrywanie). |

**4.3. Polityka Bezpieczeństwa Teleinformatycznego**

|  |  |
| --- | --- |
| Dokument | Opis / Zakres |
| Procedura przechowywania, zbierania i zarządzania logami systemowymi | Ustala zasady pozyskiwania i analizy logów (z serwerów, urządzeń sieciowych, systemów operacyjnych), ich retencji (np. minimalny czas przechowywania), a także sposób wykrywania podejrzanych aktywności. |
| Regulamin bezpieczeństwa informacji w pracy zdalnej | Zasady i wymagania dot. wykorzystywania sprzętu prywatnego lub służbowego poza siedzibą urzędu (np. VPN, szyfrowanie komunikacji, dwuskładnikowe uwierzytelnianie). Regulamin obejmuje również wskazówki dot. ochrony urządzeń mobilnych i reakcji na potencjalne zagrożenia. |
| Instrukcje szyfrowania i bezpiecznego korzystania z przeglądarki | Wytyczne dotyczące wdrażania protokołów i narzędzi szyfrujących (SSL/TLS, S/MIME, VPN), konfiguracji przeglądarek, zarządzania certyfikatami, blokowania wtyczek podnoszących ryzyko ataku. Koncentrują się na ochronie poufności i integralności przesyłanych informacji. |
| Procedura przeglądów i konserwacji systemów | Określa harmonogram i zakres regularnych prac utrzymaniowych (instalacja poprawek bezpieczeństwa, aktualizacja oprogramowania, kontrola poprawności działania usług).  |
| Raport pracy Administratora Systemów Informatycznych | Standardowy szablon dokumentu, w którym Administrator przedstawia okresowe czynności administracyjne (np. analiza logów, stanu antywirusów, aktualności certyfikatów). Umożliwia udokumentowanie i kontrolę zadań związanych z bezpieczeństwem teleinformatycznym. |
| Procedura zarządzania incydentami bezpieczeństwa informacji i cyberbezpieczeństwo | Kompleksowy opis trybu reagowania na ataki i naruszenia (phishing, ransomware, wyciek danych), obejmujący etapy zgłaszania, klasyfikacji, analizy, przeciwdziałania skutkom, a także obowiązek raportowania do organów zewnętrznych (np. CSIRT) w razie poważnych incydentów zgodnie z uoKSC. |
| Procedura kontroli dostępu | Definiuje zasady nadawania i odbierania uprawnień w systemach IT, w tym autoryzacji użytkowników, polityki haseł, wykorzystania tokenów lub kart inteligentnych. Przewiduje również sytuacje nadzwyczajne (np. udzielanie dostępu w trybie awaryjnym) i metodę kontroli skuteczności tych mechanizmów. |
| Wzór formularza ewidencji sprzętu i oprogramowania | Umożliwia bieżące śledzenie posiadanych urządzeń komputerowych (stacje robocze, laptopy, serwery, drukarki) oraz licencji na oprogramowanie. Zawiera pola na numer inwentarzowy, datę zakupu, rodzaj licencji, przypisanie do użytkownika, planowane terminy wymiany sprzętu itp. |
| Procedura szyfrowania danych | Zasady i techniki zabezpieczenia danych w spoczynku (np. szyfrowanie dysków, pendrive’ów) i w tranzycie (np. poczta elektroniczna). Obejmuje również reguły przechowywania i ochrony kluczy kryptograficznych oraz sposób postępowania w przypadku utraty klucza lub hasła. |
| Procedura zgłaszania, realizacji i testowania nowych rozwiązań informatycznych | Określenie cyklu wprowadzania nowych systemów/aplikacji (Change Management): dokumentowanie celowości, ocena ryzyka, testy bezpieczeństwa, wdrożenie produkcyjne i odbiór. Pozwala unikać nagłych wdrożeń niosących ryzyko podatności lub niedopasowania do reszty środowiska IT. |
| Procedura użytkowania poczty elektronicznej oraz korzystania z sieci Internet | Zbiór zaleceń nt. ochrony poczty przed phishingiem, spamem, złośliwym oprogramowaniem, a także wskazanie dozwolonych usług i zachowań w Internecie (np. blokada stron o podwyższonym ryzyku).  |
| Procedura utylizacji i niszczenia nośników danych | Precyzuje metody całkowitego niszczenia informacji przechowywanych na nośnikach papierowych i elektronicznych (dyski HDD, SSD, USB). Określa też protokół potwierdzający bezpowrotne i bezpieczne usunięcie danych, tak aby uniemożliwić ich odzyskanie. |
| Procedura bezpieczeństwa sieci teleinformatycznych | Zawiera zalecenia konfiguracyjne (firewalle, systemy IDS/IPS, segmentacja VLAN), sposób monitorowania ruchu sieciowego i reagowania na ataki (np. DDoS, sniffing). Uwzględnia zasady budowania bezpiecznej architektury i zarządzania punktami dostępu (Wi-Fi). |
| Procedura postępowania w zakresie wykonywania i obsługi kopii zapasowych oraz testowania nośników | Szczegółowy opis planu wykonywania backupów, ich lokalizacji (on-site/off-site), częstotliwości testów przywracania danych, sposobu dokumentowania tych testów. |
| Procedury zarządzania podatnościami | Opis cyklicznego procesu skanowania systemów i aplikacji w poszukiwaniu luk, priorytetyzacji działań naprawczych i weryfikacji poprawnego wdrożenia łatek. Powinien też odnosić się do współpracy z dostawcami/producentami w kwestiach bezpieczeństwa. |

**4.4. Polityka Ciągłości Działania**

|  |  |
| --- | --- |
| Dokument | Opis / Zakres |
| Analiza wpływu biznesowego (BIA) | Identyfikacja procesów kluczowych dla funkcjonowania jednostki, określenie maksymalnych dopuszczalnych przestojów (RTO) i tolerancji na utratę danych (RPO), a także wskazanie zasobów krytycznych (personel, systemy IT, infrastruktura). |
| Plany ciągłości działania | Szczegółowy opis procedur umożliwiających zachowanie lub szybkie przywrócenie kluczowych procesów w razie awarii, katastrofy naturalnej lub ataku cybernetycznego. Dokument uwzględnia też alternatywne miejsca pracy, sposoby komunikacji w kryzysie i priorytety w przywracaniu usług. |
| Ewidencja testowania planów ciągłości działania | Rejestr przedstawiający, w jaki sposób i jak często przeprowadzano testy planów ciągłości. Uwzględnia scenariusze symulacji, wyniki testów, zidentyfikowane niezgodności i podjęte działania doskonalące. |
| Raport ciągłości działania | Raport podsumowujący obecną dojrzałość organizacji w obszarze ciągłości działania, opisujący ewentualne incydenty, skuteczność reakcji i rekomendacje na przyszłość. Dokument stanowiący wkład w planowanie kolejnych usprawnień i strategii rozwoju SZBI. |

**V. Warunki realizacji i odbioru**

1. **Harmonogram prac**
	1. Etap analityczny (przegląd istniejących dokumentów, ocena ryzyka) powinien zostać wykonany w terminie 2 tygodni od podpisania umowy.
	2. Etap opracowania dokumentacji wraz z konsultacjami z Zamawiającym – do 4 tygodni po zakończeniu analizy.
	3. Etap wdrożenia i instruktażu – do 2 tygodni po akceptacji dokumentacji.
	4. Etap testów, przeglądu i aktualizacji – przeprowadzony w ciągu 2 tygodni od zakończenia wdrożenia (z możliwością powtarzania cyklu w ramach gwarancji)
2. **Forma przekazania dokumentacji**
	1. Dokumentacja ma być dostarczona w formie elektronicznej (format edytowalny i/lub PDF), a na życzenie Zamawiającego – także w wersji drukowanej.
	2. Wszelkie procedury powinny być oznakowane (wersjonowane), tak aby łatwo zidentyfikować najnowszą, obowiązującą wersję.
3. **Szkolenia i instruktaże**
	1. Zaleca się, by Wykonawca przedstawił Administratorowi sieci jednostki materiały szkoleniowe (np. prezentacje, skrypty) oraz metody oceny skuteczności (testy, ankiety)
4. **Odbiór końcowy i raport**
	1. Odbiór zostanie potwierdzony podpisaniem protokołu, w którym Zamawiający oświadcza, że zakres przedmiotu zamówienia został zrealizowany należycie.
	2. Wykonawca dostarczy raport podsumowujący (w formie papierowej i elektronicznej) zawierający opis wykonanych prac, ew. zalecenia i opis potencjalnych obszarów do dalszego rozwoju.

**VI. Postanowienia końcowe**

Wykonawca jest zobowiązany do zachowania w poufności wszystkich informacji, danych i dokumentów pozyskanych podczas realizacji niniejszego zamówienia; zobowiązanie to obejmuje zakaz ujawniania treści wrażliwych osobom lub podmiotom nieupoważnionym i obowiązuje także po zakończeniu współpracy, o ile przepisy prawa lub umowa nie stanowią inaczej. Z chwilą odbioru końcowych rezultatów prac wszelkie wytworzone materiały i dokumenty przechodzą na własność Zamawiającego wraz z przysługującymi im majątkowymi prawami autorskimi. W razie pojawienia się w trakcie realizacji zamówienia nowych regulacji krajowych lub unijnych, Wykonawca uwzględni te zmiany w tworzonej dokumentacji i procedurach, tak aby zapewnić ciągłą zgodność z obowiązującym prawem. Szczegółowe ustalenia dotyczące kar umownych za opóźnienia, nienależyte wykonanie przedmiotu zamówienia, czy naruszenie tajemnicy, a także zasady odpowiedzialności stron, zostaną sprecyzowane w umowie.