Opracowanie dokumentacji systemu bezpieczeństwa informacji

Minimalne składowe dokumentacji

1. **Polityka Bezpieczeństwa Informacji zawierająca**:

1.1 Procedura i instrukcje prowadzenia audytów wewnętrznych

1.2 Procedura nadzoru nad dokumentami

1.3 Procedura i instrukcja działań korygujących

1.4 Procedura postępowania z incydentami

1.5 Polityka zarządzania zasobami ludzkimi

2. **Pozostała dokumentacja SZBI**:

2.1 Pomiar efektywności zarządzania bezpieczeństwem informacji

2.2 Deklaracja stosowania zabezpieczeń według normy iso/iec 27001

2.3 Inwentaryzacja aktywów i ich właścicieli oraz zabezpieczeń

2.4 Funkcjonowanie Systemu Zarządzania Bezpieczeństwem Informacji (Przegląd stosowanych zabezpieczeń i dokumentów)

2.5 Wykaz pracowników

2.6 Analiza ryzyka (przeprowadzanie analizy + raport)

2.7 Metodyka szacowania i zarządzania ryzykiem

2.8 Plan ciągłości działania

3. **Instrukcja zarządzania systemami informatycznymi w tym instrukcje**:

3.1 Instrukcja korzystania z urządzeń mobilnych

3.2 Instrukcja pracy zdalnej

3.3 Instrukcja eksploatacji sprzętu informatycznego

3.4 Procedura kontroli dostępu

3.5 Instrukcja przydzielania i odbierania dostępów użytkownikom

3.6 Instrukcja przydzielania dostępów administracyjnych

3.7 Polityka haseł

3.8 Polityka czystego biurka i ekranu

3.9 Polityka stosowania zabezpieczeń kryptograficznych

3.10 Polityka kopii zapasowych

3.11 Zabezpieczenie systemu informatycznego przed działalnością nieuprawnionego oprogramowania

3.12 Instrukcja wykonywanie przeglądów i konserwacji systemów informatycznych

3.13 Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym

3.14 Procedura nadawania uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym

3.15 Zasady korzystania z poczty elektronicznej

3.16 Minimalne wymagania bezpieczeństwa dla systemów informatycznych

4. **Wzory dokumentów**:

4.1 Rejestr zmian

4.2 Karta przeglądu dokumentacji

4.3 Program audytów wewnętrznych

4.4 Harmonogram audytów wewnętrznych

4.5 Karta audytu wewnętrznego

4.6 Ewidencja wydanych aktywów

4.7 Powołanie audytora

4.8 Powołanie ASI

4.9 Plan audytu wewnętrznego dla stacji roboczej

4.10 Informacja o zarejestrowanych incydentach

5. **Dokumenty związane z systemem ochrony danych osobowych**

5.1 Polityka bezpieczeństwa danych osobowych

5.2 Instrukcja postepowania z incydentem bezpieczeństwa

5.3 Procedura postępowania w sytuacji naruszenia ochrony danych osobowych

5.4 Rejestr incydentów

5.5 Rejestr umów powierzania danych

5.6 Wniosek o udostępnienie danych osobowych

5.7 Rejestr udostępnionych danych osobowych

5.8 Upoważnienie do przetwarzania danych osobowych

5.9 Oświadczenie o zachowaniu tajemnicy

5.10 Ewidencja osób upoważnionych do przetwarzania danych osobowych

5.11 Wykaz miejsc przetwarzania danych osobowych

5.12 Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania

5.13 Opis struktury zbiorów danych osobowych

5.14 Sposób przepływu danych osobowych

5.15 Opis ośrodków technicznych i organizacyjnych

5.16 Wzór- powołanie ASI

5.17 Wzór- umowa o zachowanie poufności i zakazie konkurencji

5.18 Szkolenie - listy obecności, oświadczenia pracowników

Powyższa dokumentacja musi spełniać normy i przepisy zawarte w:

- KRI (Krajowe Ramy Interoperacyjności)

- PBI (Polityka bezpieczeństwa informacji)

- SZBI (System Zarządzania Bezpieczeństwem Informacji)

- NIS (Dyrektywa NIS-1,NIS-2)

- RODO (Ogólne rozporządzenie o ochronie danych osobowych)

- ISO 27001 (międzynarodowa norma standaryzująca systemy zarządzania bezpieczeństwem informacji (SZBI))

Wykonawca musi posiadać certyfikat ISO 27001