Załącznik nr 1 – Szczegółowy opis przedmiotu zamówienia

PRZEPROWADZENIE WARSZTATÓW I WDROŻENIE SZBI

W ramach warsztatów prowadzonych z osobą prowadzącą w obszarze Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) przewiduje się przegląd istniejących procedur, omówienie przykładowej dokumentacji SZBI i przygotowanie gotowej dokumentacji dla wszystkich jednostek biorących udział w warsztatach. Uczestnicy warsztatów zostaną zaangażowani w proces opracowania nowej dokumentacji, dostosowanej do specyficznych potrzeb organizacji, zgodnie z obowiązującymi normami oraz wymaganiami.

Celem warsztatów jest przekazanie praktycznej wiedzy z zakresu opracowania, ustanawiania, wdrażania, eksploatacji, monitorowania i przeglądu, a także utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji, zapewniającego poufność, dostępność i integralność informacji, z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność oraz niezawodność.

Uczestnikami warsztatów są 3 typy jednostek:

- Urząd Miejski w Gołdapi,
- Ośrodek Pomocy Społecznej w Gołdapi,
- Jednostki Oświatowe Gminy Gołdap (tj. Szkoły Podstawowe oraz Przedszkole Samorządowe) oraz Ośrodek Sportu i Rekreacji w Gołdapi.

Dokumentacja musi zawierać następujące kryteria:

1. **Ewidencja Obszaru Przetwarzania Informacji:**
   - Dokument musi zawierać ewidencję obszarów przetwarzania informacji, obejmującą lokalizacje wraz z oznaczeniami, nazwami, kondygnacjami i adresami.
   - Dokument powinien służyć do monitorowania i zarządzania miejscami, w których przetwarzane są chronione informacje.
2. **Wprowadzenie do Systemu Zarządzania Bezpieczeństwem informacji**
   - Dokument musi definiować podstawowe zasady Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym ochronę aktywów informacyjnych, monitorowanie ryzyk oraz wdrażanie zabezpieczeń.

- Dokument powinien opisywać procesy zarządzania bezpieczeństwem informacji, bazujące na cyklu PDCA (Plan-Do-Check-Act), obejmujące szacowanie ryzyka, monitorowanie skuteczności zabezpieczeń i ich doskonalenie.

3. Terminy stosowane w Systemie Zarządzania Bezpieczeństwem Informacji
   - Dokument musi zawierać definicje terminów stosowanych w Systemie Zarządzania Bezpieczeństwem Informacji (SZBI), takich jak ryzyko, aktywa informacyjne, incydent bezpieczeństwa oraz cyberbezpieczeństwo.
   - Każdy termin powinien być dokładnie opisany, uwzględniając jego znaczenie oraz zastosowanie w kontekście zarządzania bezpieczeństwem informacji.
4. Kontekst Organizacji
   - Dokument musi opisywać czynniki zewnętrzne i wewnętrzne wpływające na organizację w kontekście Systemu Zarządzania Bezpieczeństwem Informacji, w tym aspekty prawne, regulacyjne, technologiczne, społeczne oraz finansowe.
   - Dokument powinien określać zakres Systemu Zarządzania Bezpieczeństwem Informacji, uwzględniając lokalizacje, procesy, zasoby oraz jednostki organizacyjne, które są objęte systemem.
5. Zarządzanie Ryzykiem w Bezpieczeństwie informacji
   - Dokument musi opisywać proces zarządzania ryzykiem w bezpieczeństwie informacji, obejmujący identyfikację, analizę, ocenę oraz postępowanie z ryzykiem, w tym kryteria oceny ryzyka i akceptacji ryzyka.
   - Dokument powinien definiować metodykę szacowania ryzyka, w tym sposób określania prawdopodobieństwa, skutków oraz przypisywania wartości ryzyka, a także wytyczne dotyczące akceptowania, monitorowania i przeglądu ryzyka.
6. Instrukcja Szacowania i Postępowania z Ryzykiem w Bezpieczeństwie Informacji
   - Instrukcja musi opisywać proces szacowania i postępowania z ryzykiem w bezpieczeństwie informacji, obejmujący identyfikację zagrożeń, podatności oraz aktywów i ich zabezpieczeń, których ryzyko dotyczy.
   - Dokument powinien zawierać szczegółowe wytyczne dotyczące analizy ryzyka, w tym oszacowanie następstw, prawdopodobieństwa, poziomów ryzyka oraz metody określania i dokumentowania działań w zakresie postępowania z ryzykiem.
7. Działania odnoszące się do Ryzyk i Szans Systemu Zarządzania Bezpieczeństwem Informacji.
   - Dokument musi opisywać działania odnoszące się do zidentyfikowanych ryzyk i szans w Systemie Zarządzania Bezpieczeństwem Informacji, w tym określenie sposobów realizacji działań oraz ich integrację z procesami SZBI.

- Dokument powinien zawierać wytyczne dotyczące oceny skuteczności działań, uwzględniając monitorowanie, pomiary, audyty oraz przeglądy zarządzania, aby zapewnić zgodność z wymaganiami prawnymi oraz bezpieczeństwo informacji.

8. Deklaracja Stosowania Opracowana
   - Dokument musi zawierać wykaz zabezpieczeń stosowanych w Systemie Zarządzania Bezpieczeństwem Informacji, wraz z uzasadnieniem ich wyboru oraz oceną wdrożenia lub wyłączenia, zgodnie z Załącznikiem A normy ISO/IEC 27001.
   - Dokument powinien opisywać sposób wdrożenia zabezpieczeń, wskazując ich cel, specyfikę działalności oraz wyniki analizy ryzyka, a także uzasadniać ewentualne wyłączenia zabezpieczeń.
9. Cele bezpieczeństwa informacji
   - Dokument musi określać cele bezpieczeństwa informacji, które obejmują zarządzanie ryzykiem, incydentami, zgodność z przepisami oraz zapewnienie ciągłości działania i bezpieczeństwa aktywów.
   - Dokument powinien zawierać mierzalne wskaźniki realizacji celów, w tym liczbę audytów, szkoleń, zgłoszeń incydentów, a także utrzymywanie odpowiednich rejestrów i ewidencji aktywów.
10. Plan osiągniecia Celów Bezpieczeństwa Informacji
    - Dokument musi zawierać plan realizacji celów bezpieczeństwa informacji, określając zadania, wskaźniki oraz harmonogram ich realizacji i weryfikacji, zgodnie z raportami z monitorowania i pomiarów systemu zarządzania bezpieczeństwem informacji.
    - Plan powinien przypisywać odpowiedzialność za realizację poszczególnych zadań oraz wskazywać kluczowe cele, takie jak zarządzanie ryzykiem, incydentami, ciągłością działania oraz zgodność z wymaganiami prawnymi i regulacyjnymi.
11. Monitorowanie, Pomiary, Analiza i Ocena Systemu Zarządzania Bezpieczeństwem Informacji
    - Dokument musi opisywać proces monitorowania, pomiarów, analizy i oceny Systemu Zarządzania Bezpieczeństwem Informacji, obejmujący zgodność z wymaganiami prawnymi oraz skuteczność w osiąganiu celów bezpieczeństwa informacji.
    - Dokument powinien zawierać wskaźniki monitorowania oraz określać odpowiedzialność Pełnomocnika ds. Bezpieczeństwa Informacji za utrzymywanie raportów i ich przekazywanie Najwyższemu Kierownictwu.
12. Raport z Monitorowania, Pomiarów, Analizy i Oceny Systemu Zarządzania Bezpieczeństwem informacji
    - Raport musi zawierać wyniki monitorowania, pomiarów, analizy i oceny Systemu Zarządzania Bezpieczeństwem Informacji, w tym liczbę audytów, działań zaradczych, incydentów oraz wskaźniki ryzyka i zgodności z wymaganiami prawnymi.

- Dokument powinien zawierać przegląd zapisów i wskaźników monitorowania z poprzedniego roku oraz przypisywać odpowiedzialność za realizację poszczególnych działań związanych z zarządzaniem bezpieczeństwem informacji.

13. Raport z Audytu Wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji
    - Raport z audytu wewnętrznego musi zawierać ocenę zgodności Systemu Zarządzania Bezpieczeństwem Informacji z wymaganiami prawnymi i regulacyjnymi, a także oceniać jego skuteczność w osiąganiu zamierzonych celów.
    - Dokument powinien przedstawiać ustalenia audytu, w tym wykryte zgodności i niezgodności, dowody potwierdzające oraz zalecenia audytora dotyczące doskonalenia systemu.
14. Audyty Wewnętrzne Systemu Zarządzania Bezpieczeństwem Informacji
    - Dokument musi definiować zasady i procedury przeprowadzania audytów wewnętrznych Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z normami ISO oraz wymogami prawnymi, w tym zasady rzetelności, poufności, niezależności i podejścia opartego na dowodach.
    - Dokument powinien opisywać zarządzanie programem audytów, w tym jego tworzenie, zatwierdzanie, przygotowanie planów audytów, przeprowadzanie działań audytowych oraz działania poaudytowe, wraz z odpowiedzialnością za realizację i doskonalenie audytów.
15. Plan Audytu Wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji.
    - Plan Audytu Wewnętrznego musi określać cele, zakres, kryteria oraz metody przeprowadzania audytu, w tym audyty na miejscu i zdalne, a także analizę dokumentów, obserwację pracy i rozmowy z personelem.
    - Dokument powinien zawierać informacje o odpowiednich wymaganiach prawnych i regulacyjnych, procesach do audytu, oraz wskazywać lokalizacje i osoby odpowiedzialne za poszczególne etapy audytu.
16. Program Audytów Wewnętrznych Systemu Zarządzania Bezpieczeństwem Informacji
    - Program Audytów Wewnętrznych musi zawierać liczbę i rodzaje zaplanowanych audytów, ich cele, zakres oraz kryteria, zgodnie z wymaganiami prawnymi i regulacyjnymi dotyczącymi Systemu Zarządzania Bezpieczeństwem Informacji.
    - Dokument powinien definiować metody audytu, takie jak wizyty, przegląd dokumentów, rozmowy oraz analizę danych, a także przypisywać odpowiedzialność za realizację audytów Pełnomocnikowi ds. Bezpieczeństwa Informacji.

17. Przegląd Zarządzania
    - Dokument Przegląd Zarządzania musi zawierać coroczną ocenę przydatności, adekwatności i skuteczności Systemu Zarządzania Bezpieczeństwem Informacji, w tym analizę działań korygujących, doskonalących oraz wdrożonych w wyniku incydentów i audytów wewnętrznych.
    - Dokument powinien obejmować przegląd zmian czynników zewnętrznych i wewnętrznych, analizę wyników monitorowania systemu, cele bezpieczeństwa oraz informacje zwrotne od stron zainteresowanych.
18. Raport z Przeglądu Zarządzania
    - Raport z Przeglądu Zarządzania musi zawierać ocenę działań podjętych po wcześniejszych przeglądach zarządzania, analizę czynników zewnętrznych i wewnętrznych oraz informacje o działaniach korygujących i doskonalących w obszarze bezpieczeństwa informacji.
    - Dokument powinien obejmować wyniki audytów wewnętrznych, analizę celów bezpieczeństwa informacji, a także możliwości doskonalenia systemu wynikające z raportów oraz przeglądów.
19. Doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji
    - Dokument musi opisywać procedury identyfikacji, korygowania i doskonalenia niezgodności w Systemie Zarządzania Bezpieczeństwem Informacji, w tym działania eliminujące przyczyny niezgodności oraz ocenę skuteczności wdrożonych środków korygujących.
    - Dokument powinien obejmować proces ciągłego doskonalenia systemu poprzez regularne przeglądy, monitorowanie, analizę oraz raportowanie działań doskonalących i korygujących.
20. Polityka Bezpieczeństwa Informacji
    - Polityka Bezpieczeństwa Informacji musi określać ogólne kierunki i wytyczne w zakresie ochrony informacji, w tym zarządzanie poufnością, integralnością, dostępnością oraz innymi atrybutami bezpieczeństwa, takimi jak autentyczność, rozliczalność i niezaprzeczalność.
    - Dokument powinien obejmować zasady zarządzania ryzykiem, incydentami oraz ciągłością bezpieczeństwa informacji, a także uwzględniać wymagania prawne, regulacyjne i umowne, zgodnie z przyjętymi celami bezpieczeństwa informacji.
21. Raport z Przeglądu Udokumentowanych Informacji Systemu Zarządzania Bezpieczeństwem Informacji
    - Raport z Przeglądu Udokumentowanych Informacji musi obejmować ocenę zgodności udokumentowanych informacji Systemu Zarządzania Bezpieczeństwem Informacji, zidentyfikowane modyfikacje oraz propozycje aktualizacji w przypadku stwierdzenia potrzeby zmiany.
    - Dokument powinien zawierać przegląd poszczególnych polityk, procedur, rejestrów i planów, w tym propozycje aktualizacji wynikające z analizy ryzyk, audytów wewnętrznych i przeglądów zarządzania.

22. Rejestr Właścicieli Udokumentowanych Informacji Systemu Zarządzania Bezpieczeństwem Informacji
    - Rejestr Właścicieli Udokumentowanych Informacji musi zawierać wykaz dokumentów Systemu Zarządzania Bezpieczeństwem Informacji wraz z przypisanymi do nich właścicielami, odpowiedzialnymi za ich utrzymanie, aktualizację i zgodność z systemem.
    - Dokument powinien wskazywać funkcje i stanowiska osób odpowiedzialnych za poszczególne udokumentowane informacje, aby zapewnić nadzór i odpowiedzialność nad ich prawidłowym zarządzaniem.
23. Role, Odpowiedzialność i Uprawnienia w Systemie Zarządzania Bezpieczeństwem Informacji
    - Dokument musi definiować role, odpowiedzialność i uprawnienia związane z zarządzaniem bezpieczeństwem informacji, w tym Najwyższe Kierownictwo, Pełnomocnika ds. Bezpieczeństwa Informacji, Inspektora Ochrony Danych, Administratora Systemów Informatycznych oraz inne osoby przetwarzające informacje.
    - Dokument powinien określać obowiązki związane z nadzorem nad zarządzaniem ryzykiem, incydentami, bezpieczeństwem aktywów, a także zobowiązania do raportowania, przeglądów i doskonalenia systemu zarządzania bezpieczeństwem informacji.
24. Polityka Stosowana Urządzeń Mobilnych
    - Polityka Stosowania Urządzeń Mobilnych musi określać zasady zarządzania i zabezpieczania urządzeń mobilnych oraz zewnętrznych nośników danych, w tym autoryzację ich użytkowania poza organizacją, zgodnie z wymaganiami Polityki Zarządzania Aktywami.
    - Dokument powinien zawierać wytyczne dotyczące ochrony informacji przechowywanych w urządzeniach mobilnych, w tym ich szyfrowania, zabezpieczania przed utratą, kradzieżą lub nieuprawnionym dostępem, zgodnie z Polityką Kryptografii i innymi regulacjami bezpieczeństwa.
25. Polityka Pracy Zdalnej
    - Polityka Pracy Zdalnej musi określać zasady świadczenia pracy zdalnej, w tym wytyczne dotyczące zabezpieczenia aktywów oraz informacji przetwarzanych poza siedzibą organizacji, zgodnie z wymaganiami prawnymi i regulacyjnymi.
    - Dokument powinien zawierać wytyczne dotyczące kontroli bezpieczeństwa, użycia narzędzi pracy oraz odpowiednich zabezpieczeń technicznych i organizacyjnych, zapewniając ochronę danych osobowych oraz tajemnic prawnie chronionych.
26. Polityka Bezpieczeństwa Zasobów Ludzkich
    - Polityka Bezpieczeństwa Zasobów Ludzkich musi określać zasady zarządzania personelem w zakresie bezpieczeństwa informacji, w tym procesy rekrutacji, szkolenia, świadomości oraz procedury postępowania przed, w trakcie i po zakończeniu zatrudnienia.

- Dokument powinien zawierać wytyczne dotyczące weryfikacji kandydatów, nadawania i odbierania uprawnień, zarządzania incydentami bezpieczeństwa oraz zobowiązań personelu do przestrzegania zasad bezpieczeństwa informacji, także po zakończeniu zatrudnienia.

27. Wniosek o Nadanie, Zmianę lub Odebranie Dostępu do Systemów Informatycznych
    - Wniosek o Nadanie, Zmianę lub Odebranie Dostępu do Systemów Informatycznych musi zawierać dane dotyczące systemów informatycznych, w tym nazwę systemu, identyfikator użytkownika oraz dane uwierzytelniające, a także określać rodzaj wnioskowanej operacji (nadanie, zmiana, odebranie dostępu).
    - Dokument powinien być zatwierdzany przez kierującego jednostką organizacyjną oraz Administratora Systemów Informatycznych, potwierdzając nadanie, zmianę lub odebranie dostępu do wskazanych systemów.
28. Oświadczenie o Przestrzeganiu Wymagań Dotyczących Bezpieczeństwa Informacji
    - Oświadczenie o Przestrzeganiu Wymagań Dotyczących Bezpieczeństwa Informacji musi zobowiązywać pracowników do przestrzegania wymagań prawnych, regulacyjnych i umownych dotyczących bezpieczeństwa informacji, w tym ochrony danych osobowych.
    - Dokument powinien określać obowiązek stosowania środków technicznych i organizacyjnych, zgłaszania incydentów oraz zachowania poufności przetwarzanych informacji, także po zakończeniu współpracy.
29. Upoważnienie do Przetwarzania Informacji
    - Upoważnienie do Przetwarzania Informacji musi zawierać dane osoby upoważnionej, stanowisko, funkcję oraz zakres przetwarzania informacji, w tym procesy i cele przetwarzania, a także daty obowiązywania upoważnienia.
    - Dokument powinien być podpisany przez osobę upoważniającą oraz osobę upoważnioną, potwierdzając wydanie i odbiór upoważnienia, a wszelkie wcześniejsze upoważnienia tracą ważność.
30. Polityka Zarządzania Aktywami
    - Polityka Zarządzania Aktywami musi definiować zasady inwentaryzacji, klasyfikacji oraz odpowiedzialności za aktywa organizacji, w tym identyfikację właścicieli aktywów i procedury zarządzania nimi w celu zapewnienia ich ochrony.
    - Dokument powinien zawierać wytyczne dotyczące bezpiecznego użytkowania, przechowywania oraz wycofywania aktywów, w tym nośników informacji, zgodnie z wymaganiami prawnymi i regulacyjnymi.

31. Ewidencja Aktywów Podstawowych
    - Ewidencja Aktywów Podstawowych musi zawierać identyfikację procesów, ich właścicieli oraz szczegółowe dane na temat rodzaju i typów procesów, w tym cele przetwarzania informacji, źródła danych, metody monitorowania oraz kontrolowania przebiegu procesów.
    - Dokument powinien zawierać opisy mierników wejściowych i wyjściowych oraz określać powiązania między procesami, wskazując na ich wpływ i zależności, a także odpowiedzialność za nadzór nad aktywami i ich bezpieczeństwo.
32. Ewidencja Obszaru Przetwarzania Informacji
    - Ewidencja Obszaru Przetwarzania Informacji musi zawierać oznaczenia, lokalizacje, kondygnacje oraz adresy fizycznych miejsc, w których przetwarzane są informacje w ramach Systemu Zarządzania Bezpieczeństwem Informacji.
    - Dokument powinien umożliwiać identyfikację obszarów przetwarzania informacji, co pozwala na ich ewidencjonowanie i nadzór nad bezpieczeństwem fizycznym przetwarzanych danych.
33. Polityka Kontroli Dostępu
    - Polityka Kontroli Dostępu musi definiować zasady autoryzacji i ograniczania dostępu do aktywów oraz informacji, zgodnie z wymaganiami prawnymi, regulacyjnymi i umownymi, aby zapewnić, że dostęp mają tylko uprawnieni użytkownicy.
    - Dokument powinien obejmować procedury bezpiecznego logowania, zarządzania hasłami, kontrolę dostępu do systemów i aplikacji oraz odpowiedzialność użytkowników za poufne informacje uwierzytelniające.
34. Wymagania w Dostępie do Aktywów dla Personelu
    - Dokument Wymagania w Dostępie do Aktywów dla Personelu musi określać zasady przyznawania dostępu do aktywów wyłącznie dla uprawnionych osób, zgodnie z nadanymi upoważnieniami oraz zabezpieczeniami wdrożonymi w organizacji.
    - Dokument powinien zawierać wytyczne dotyczące zabezpieczania nośników informacji, stosowania polityki czystego biurka i ekranu, a także obowiązek zgłaszania incydentów bezpieczeństwa zgodnie z Polityką Zarządzania Incydentami.
35. Wymagania w Dostępie do Aktywów dla Podmiotów Zewnętrznych
    - Dokument Wymagania w Dostępie do Aktywów dla Podmiotów Zewnętrznych musi określać zasady dostępu podmiotów zewnętrznych do aktywów organizacji, ograniczając dostęp do zakresu niezbędnego do realizacji określonych działań zgodnie z umowami, w tym Umowami o Zachowaniu Poufności oraz Umowami Przetwarzania Danych Osobowych.

- Dokument powinien zawierać wytyczne dotyczące nadzoru nad przetwarzaniem informacji przez podmioty zewnętrzne oraz obowiązek zgłaszania wszelkich stwierdzonych lub domniemanych nieprawidłowości związanych z przetwarzaniem aktywów.

36. Procedura Dostępu do Sieci i Usług Sieciowych
    - Procedura Dostępu do Sieci i Usług Sieciowych musi określać zasady przyznawania dostępu do sieci i usług sieciowych wyłącznie uprawnionym użytkownikom, zgodnie z wymaganiami dotyczącymi identyfikacji, uwierzytelniania i autoryzacji.
    - Dokument powinien zawierać wytyczne dotyczące sposobów dostępu, takich jak sieci przewodowe, bezprzewodowe, VPN, oraz połączenia zdalne, a także nadzór nad połączeniami przez Administratora Systemów Informatycznych.
37. Procedura Zarządzania Dostępem Użytkowników
    - Procedura Zarządzania Dostępem Użytkowników musi określać zasady rejestrowania, wyrejestrowywania, przydzielania i odbierania praw dostępu użytkownikom systemów informatycznych, zgodnie z upoważnieniami oraz Wnioskami o Nadanie, Zmianę lub Odebranie Dostępu.
    - Dokument powinien zawierać wytyczne dotyczące zarządzania prawami uprzywilejowanego dostępu, przeglądów praw dostępu użytkowników oraz bezpiecznego przydzielania poufnych informacji uwierzytelniających.
38. Instrukcja Szyfrowania Informacji w Postaci Cyfrowej z Wykorzystaniem Aplikacji 7-Zip
    - Instrukcja musi opisywać proces szyfrowania informacji w postaci cyfrowej przy użyciu aplikacji 7-Zip, w tym instalację oprogramowania oraz procedurę szyfrowania plików z zastosowaniem odpowiednich zabezpieczeń.
    - Dokument powinien zawierać wytyczne dotyczące tworzenia bezpiecznych haseł zgodnie z Zasadami Tworzenia i Postępowania z Hasłami oraz sposób odszyfrowania plików przy użyciu właściwego hasła.
39. Polityka Kryptografii
    - Polityka Kryptografii musi określać zasady stosowania kryptografii do ochrony poufności, autentyczności i integralności informacji, w tym wymagania dotyczące szyfrowania informacji na nośnikach wymiennych i urządzeniach przenośnych.
    - Dokument powinien zawierać wytyczne dotyczące zarządzania kluczami kryptograficznymi, w tym ich generowanie, przechowywanie, archiwizowanie, dystrybucję oraz bezpieczne niszczenie po wycofaniu z użytku.

40. Polityka Bezpieczeństwa Fizycznego i Środowiskowego
    - Polityka Bezpieczeństwa Fizycznego i Środowiskowego musi określać zasady zabezpieczania obszarów, w których przetwarzane są informacje, w tym zabezpieczenia wejść, ochronę przed zagrożeniami zewnętrznymi i środowiskowymi oraz kontrolę dostępu do obszarów bezpiecznych.
    - Dokument powinien zawierać wytyczne dotyczące ochrony sprzętu, monitorowania warunków środowiskowych, bezpieczeństwa okablowania oraz zasad wynoszenia i zbywania aktywów, w tym stosowanie polityki czystego biurka i czystego ekranu.
41. Polityka Bezpiecznej Eksploatacji
    - Polityka Bezpiecznej Eksploatacji musi definiować zasady bezpiecznej eksploatacji systemów informacyjnych, w tym dokumentowanie procedur operacyjnych, zarządzanie zmianami oraz monitorowanie wydajności i pojemności systemów.
    - Dokument powinien obejmować wytyczne dotyczące ochrony przed szkodliwym oprogramowaniem, rejestrowania zdarzeń, zarządzania kopią zapasową oraz odpowiedzialności za instalację, konserwację i audyt systemów informacyjnych.
42. Czynności Zabronione
    - Dokument "Czynności Zabronione" musi zawierać wykaz działań niedozwolonych w zakresie przetwarzania informacji, takich jak nieujawnianie haseł, niewykorzystywanie nieautoryzowanego oprogramowania oraz obowiązek stosowania polityki czystego biurka i ekranu.
    - Dokument powinien określać zasady ochrony urządzeń przed nieuprawnionym dostępem, zakaz używania tego samego hasła w wielu systemach oraz obowiązek szyfrowania chronionych informacji na nośnikach danych i podczas ich przesyłania.
43. Procedura Instalacji i Konfiguracji Systemów Informacyjnych
    - Procedura Instalacji i Konfiguracji Systemów Informacyjnych musi definiować zasady instalacji i konfiguracji oprogramowania oraz sprzętu komputerowego przez Administratora Systemów Informatycznych lub inny upoważniony personel, uwzględniając wymagania bezpieczeństwa wynikające z polityk organizacji.
    - Dokument powinien zawierać wytyczne dotyczące zarządzania zmianami oprogramowania, utrzymywania poprzednich wersji oraz nadzoru nad dostępem serwisantów dostawców, aby zapobiegać incydentom związanym z bezpieczeństwem informacji.
44. Procedura Konserwacji i Napraw Urządzeń Komputerowych
    - Procedura Konserwacji i Napraw Urządzeń Komputerowych musi definiować zasady wykonywania konserwacji i napraw urządzeń komputerowych przez Administratora Systemów Informatycznych lub podmioty zewnętrzne, zgodnie z warunkami określonymi przez producenta.

- Dokument powinien zawierać wytyczne dotyczące nadzoru nad naprawami realizowanymi przez podmioty zewnętrzne oraz obowiązek usunięcia nośników danych lub informacji przed przekazaniem urządzeń do serwisu zewnętrznego.

45. Procedura Obsługi Nośników Informacji
    - Procedura Obsługi Nośników Informacji musi określać zasady ochrony nośników informacji przed ich utratą, zniszczeniem, nieuprawnionym odczytem oraz modyfikacją, zarówno dla nośników analogowych, jak i cyfrowych.
    - Dokument powinien zawierać wytyczne dotyczące niszczenia uszkodzonych nośników danych, trwałego usuwania informacji przed przekazaniem nośników innym osobom lub podmiotom oraz zgodności z Polityką Zarządzania Aktywami.
46. Procedura Użytkowania Systemów Informacyjnych
    - Procedura Użytkowania Systemów Informacyjnych musi definiować zasady korzystania z systemów informacyjnych wyłącznie przez uprawniony personel, zgodnie z przydzielonymi upoważnieniami oraz Polityką Kontroli Dostępu, obejmując autoryzację i uwierzytelnianie.
    - Dokument powinien zawierać wytyczne dotyczące odpowiedzialności użytkowników za poufność danych uwierzytelniających, zgłaszanie awarii oraz zgodność użytkowania z warunkami określonymi przez organizację
47. Procedura uruchamiania i Zatrzymania Komputera
    - Procedura Uruchamiania i Zatrzymania Komputera musi definiować zasady prawidłowego uruchamiania komputera, w tym sprawdzenie połączeń, włączanie zasilania oraz proces uwierzytelniania użytkownika przy dostępie do systemu operacyjnego.
    - Dokument powinien zawierać wytyczne dotyczące bezpiecznego zamykania systemu, odłączania urządzeń przenośnych oraz wyłączania komputera, zabraniając wyłączania poprzez bezpośrednie użycie przycisku zasilania poza sytuacjami awaryjnymi
48. Zasady Tworzenia i Postępowania z Hasłami
    - Dokument "Zasady Tworzenia i Postępowania z Hasłami" musi definiować wytyczne dotyczące tworzenia silnych haseł, ich długości (minimum 16 znaków) oraz stosowania wieloskładnikowego uwierzytelniania (MFA) tam, gdzie to możliwe.
    - Dokument powinien zawierać zasady poufności haseł, zakaz ich zapisywania w przeglądarkach, wymóg regularnej zmiany haseł co 90 dni oraz zakaz używania tych samych haseł w różnych systemach informatycznych.

49. Polityka Zarządzania Bezpieczeństwem Sieci
    - Polityka Zarządzania Bezpieczeństwem Sieci musi definiować zasady ochrony sieci organizacji, w tym zarządzanie urządzeniami sieciowymi, stosowanie zapór sieciowych, monitorowanie oraz uwierzytelnianie dostępu do sieci.
    - Dokument powinien zawierać wytyczne dotyczące rozdzielania (segmentacji) sieci, bezpieczeństwa usług sieciowych oraz mechanizmów uwierzytelniania, szyfrowania i ograniczania dostępu do usług, zgodnie z umowami SLA i najlepszymi praktykami.
50. Polityka Przesyłania Informacji
    - Polityka Przesyłania Informacji musi definiować zasady ochrony informacji przesyłanych wewnątrz organizacji oraz do podmiotów zewnętrznych, w tym wymóg stosowania ochrony kryptograficznej i zabezpieczeń przed złośliwym oprogramowaniem.
    - Dokument powinien zawierać wytyczne dotyczące zawierania porozumień w zakresie przesyłania chronionych informacji, określających środki komunikacji, nadawców, odbiorców oraz mechanizmy ochrony danych.
51. Zasady korzystania z poczty Elektronicznej
    - Zasady Korzystania z Poczty Elektronicznej muszą definiować zasady przesyłania informacji chronionych, w tym wymóg stosowania kryptografii i podpisów elektronicznych, gdy wymaga tego prawo lub procedury organizacji.
    - Dokument powinien zawierać wytyczne dotyczące korzystania z poczty elektronicznej wyłącznie w celach służbowych, zakaz używania prywatnej poczty elektronicznej na urządzeniach organizacji oraz zasady bezpiecznego postępowania z załącznikami i odnośnikami od nieznanych nadawców.
52. Zasady Korzystania z Internetu
    - Zasady Korzystania z Internetu muszą definiować korzystanie z Internetu wyłącznie w celach służbowych, z zakazem pobierania i instalowania nieautoryzowanych plików oraz aplikacji, a także zakazem korzystania z zasobów o treściach przestępczych, pornograficznych lub zakazanych.
    - Dokument powinien zawierać wytyczne dotyczące stosowania szyfrowanych połączeń (HTTPS), zakaz używania funkcji autouzupełniania i zapamiętywania haseł w przeglądarkach oraz obowiązek zgłaszania nieprawidłowości do Administratora Systemów Informatycznych.
53. Umowa o Zachowaniu Poufności
    - Umowa o Zachowaniu Poufności musi określać zasady ochrony informacji chronionych prawnie, zobowiązując Strony do przetwarzania tych informacji zgodnie z przepisami prawa, wymaganiami regulacyjnymi oraz umownymi, wyłącznie przez upoważniony personel.

- Dokument powinien zawierać wytyczne dotyczące odpowiedzialności za naruszenie poufności, w tym kary umowne i odszkodowania, a także okres obowiązywania zobowiązania do zachowania poufności po zakończeniu realizacji celu umowy.

54. Wymagania Związane z Bezpieczeństwem Systemów Informacji
    - Wymagania Związane z Bezpieczeństwem Systemów Informacyjnych muszą obejmować zasady zabezpieczania systemów informacyjnych na każdym etapie ich cyklu życia, w tym identyfikację użytkowników, autoryzację, rejestrowanie działań oraz zarządzanie ryzykiem.
    - Dokument powinien zawierać wytyczne dotyczące ochrony usług aplikacyjnych w sieciach publicznych, stosowania kryptografii oraz zabezpieczania transakcji, zapewniając poufność, integralność i dostępność przetwarzanych informacji.
55. Polityka bezpieczeństwa Informacji w Procesach Rozwoju i Wsparcia
    - Polityka Bezpieczeństwa w Procesach Rozwoju i Wsparcia musi definiować zasady wprowadzania bezpieczeństwa informacji w całym cyklu życia systemów informacyjnych, w tym podczas prac rozwojowych, testowania i wdrożenia systemów.
    - Dokument powinien zawierać wytyczne dotyczące bezpiecznego programowania, zarządzania zmianami w systemach, kontroli wersji oraz testów bezpieczeństwa, zarówno wewnętrznych, jak i zleconych podmiotom zewnętrznym.
56. Wymagania dotyczące Ochrony Danych Testowych
    - Wymagania Dotyczące Ochrony Danych Testowych muszą określać zasady doboru, ochrony i nadzoru nad danymi używanymi w procesach testowych, minimalizując użycie rzeczywistych danych osobowych lub chronionych informacji.
    - Dokument powinien zawierać wytyczne dotyczące stosowania procedur kontroli dostępu w środowiskach testowych oraz obowiązek usuwania rzeczywistych danych po zakończeniu testów.
57. Polityka Bezpieczeństwa Informacji w Relacjach z Dostawcami
    - Polityka Bezpieczeństwa Informacji w Relacjach z Dostawcami musi określać wymagania związane z bezpieczeństwem informacji w relacjach z dostawcami, w tym zobowiązanie do ochrony poufności, integralności i dostępności aktywów organizacji.
    - Dokument powinien zawierać wytyczne dotyczące monitorowania i kontroli dostępu dostawców do informacji, zarządzania ryzykiem związanym z łańcuchem dostaw technologii informacyjnych oraz zapewnienia odpowiedniego poziomu bezpieczeństwa w umowach z dostawcami.
58. Zarządzanie Bezpieczeństwem Informacji przez Dostawcę
    - Dokument Zarządzanie Bezpieczeństwem Informacji przez Dostawcę musi zawierać szczegółową ankietę oceniającą dostawcę pod kątem zgodności z wymaganiami dotyczącymi bezpieczeństwa

informacji, w tym stosowania polityk ochrony danych osobowych, zarządzania ryzykiem oraz incydentami cyberbezpieczeństwa.

- Dokument powinien obejmować pytania dotyczące wdrożenia systemu zarządzania bezpieczeństwem informacji, zarządzania dostępem, szyfrowania oraz przestrzegania zasad „Privacy by design" i „Privacy by default".

59. Procedura zakupu Oprogramowania i Urządzeń Komputerowych oraz Usług IT
    - Procedura Zakupu Oprogramowania i Urządzeń Komputerowych oraz Usług IT musi definiować zasady inicjowania, realizacji i weryfikacji zakupów oprogramowania, urządzeń komputerowych oraz usług IT, w tym wymagania dotyczące bezpieczeństwa informacji zgodne z regulacjami prawnymi i wewnętrznymi.
    - Dokument powinien zawierać wytyczne dotyczące sporządzania wniosku o zakup, który musi uwzględniać specyfikacje techniczne, planowane zabezpieczenia, potencjalnych dostawców oraz wymagania dotyczące bezpieczeństwa informacji i danych osobowych.
60. Polityka Zarządzania Incydentami, Zdarzeniami, Niezgodnościami i Słabościami
    - Polityka Zarządzania Incydentami, Zdarzeniami, Niezgodnościami i Słabościami musi określać zasady postępowania w przypadku incydentów związanych z bezpieczeństwem informacji, w tym ich zgłaszania, oceny, podejmowania decyzji oraz działań zaradczych i korygujących.
    - Dokument powinien zawierać wytyczne dotyczące zgłaszania naruszeń danych osobowych do odpowiednich organów w terminie nie dłuższym niż 72 godziny oraz procedury reagowania na incydenty cyberbezpieczeństwa zgodnie z wymogami prawnymi.
61. Zgłoszenie Incydentu, Zdarzenia, Niezgodności, Słabości
    - Dokument "Zgłoszenie Incydentu, Zdarzenia, Niezgodności, Słabości" musi umożliwiać zgłaszanie incydentów bezpieczeństwa, zdarzeń, niezgodności z wymaganiami regulacyjnymi oraz słabości w zabezpieczeniach, obejmując opis istoty problemu, aktywów i procesów, których dotyczy.
    - Formularz powinien zawierać szczegółowe wytyczne dotyczące dat i okoliczności incydentu, przyczyn jego wystąpienia, rodzaju naruszenia (np. ujawnienie informacji, utrata danych) oraz dane zgłaszającego, świadków i sprawców, umożliwiając anonimowe zgłoszenia.
62. Rejestr Incydentów, Zdarzeń, Niezgodności, Słabości, Działań Zaradczych, Korygujących i Doskonalących
    - Rejestr Incydentów, Zdarzeń, Niezgodności, Słabości, Działań Zaradczych, Korygujących i Doskonalących musi zawierać szczegółowy zapis wszystkich incydentów, zdarzeń, niezgodności oraz słabości dotyczących bezpieczeństwa informacji, wraz z datą, opisem problemu oraz podjętymi działaniami.

- Dokument powinien umożliwiać śledzenie działań zaradczych, korygujących i doskonalących, mających na celu poprawę poziomu bezpieczeństwa informacji oraz eliminację zidentyfikowanych problemów.

63. Polityka Ciągłości Bezpieczeństwa Informacji
    - Polityka Ciągłości Bezpieczeństwa Informacji musi definiować zasady zapewnienia ciągłości bezpieczeństwa informacji, uwzględniając planowanie, wdrożenie i utrzymanie procesów oraz środków gwarantujących bezpieczeństwo informacji w przypadku zakłóceń, takich jak incydenty czy katastrofy.
    - Dokument powinien zawierać wytyczne dotyczące tworzenia planów zarządzania ciągłością działania oraz odtwarzania po katastrofie, weryfikacji zdolności organizacji do zapewnienia ciągłości oraz nadmiarowości zasobów przetwarzania informacji.
64. Ewidencja Aktywów Wspierających Zapewniających Utrzymanie Procesów Krytycznych po Katastrofie
    - Ewidencja Aktywów Wspierających Zapewniających Utrzymanie Procesów Krytycznych po Katastrofie musi zawierać identyfikację i szczegółowy opis aktywów niezbędnych do utrzymania ciągłości procesów krytycznych, takich jak pomieszczenia, sprzęt, urządzenia komputerowe, oprogramowanie, nośniki informacji oraz personel.
    - Dokument powinien określać minimalne zasoby, w tym powierzchnię, rodzaj sprzętu, liczbę pracowników oraz wymagania dotyczące sieci, niezbędne do realizacji procesów po wystąpieniu katastrofy.
65. Plan Zarządzania Ciągłością Działania
    - Plan Zarządzania Ciągłością Działania musi określać zasady postępowania w przypadku zakłóceń procesów krytycznych, w tym procedury odzyskiwania i przywracania działania urządzeń, oprogramowania, sieci, personelu oraz lokalizacji przetwarzania informacji.
    - Dokument powinien zawierać wytyczne dotyczące Recovery Time Objective (RTO), Recovery Point Objective (RPO), maksymalnego tolerowanego okresu zakłócenia (MTPD) oraz minimalnego poziomu działalności (MBCO), niezbędnych do zapewnienia ciągłości działania.
66. Plan Zarządzania Odtwarzaniem po Katastrofie
    - Plan Zarządzania Odtwarzaniem po Katastrofie musi zawierać zasady przywracania krytycznych procesów organizacji po katastrofie, w tym identyfikację i zabezpieczenie niezbędnych aktywów, takich jak budynki, sprzęt komputerowy, oprogramowanie, nośniki danych oraz personel.
    - Dokument powinien określać rodzaje katastrof, takich jak klęski żywiołowe, awarie techniczne, ataki terrorystyczne, oraz procedury reagowania, obejmujące zapewnienie zasobów zastępczych oraz nadzorowanie realizacji planów odtwarzania.

67. Polityka Zgodności
    - Polityka Zgodności musi określać zasady monitorowania i przestrzegania wymagań prawnych, regulacyjnych oraz umownych związanych z bezpieczeństwem informacji, w tym ochronę praw własności intelektualnej oraz prywatności danych osobowych.
    - Dokument powinien zawierać wytyczne dotyczące regularnych przeglądów zgodności, w tym niezależnych audytów oraz przeglądów technicznych systemów informacyjnych, w celu zapewnienia zgodności z politykami bezpieczeństwa i standardami.
68. Informacje o Przetwarzaniu Danych Osobowych Zbieranych bezpośrednio
    - Dokument "Informacje o Przetwarzaniu Danych Osobowych Zbieranych Bezpośrednio" musi określać zasady informowania osób, których dane są przetwarzane, o celach, podstawach prawnych, odbiorcach oraz czasie przechowywania danych osobowych, zgodnie z przepisami RODO.
    - Dokument powinien zawierać wytyczne dotyczące praw osób, których dane dotyczą, takich jak prawo do dostępu, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu wobec przetwarzania oraz cofnięcia zgody na przetwarzanie danych osobowych.
69. Informacje o Przetwarzaniu Danych Osobowych Zbieranych Pośrednio
    - Dokument "Informacje o Przetwarzaniu Danych Osobowych Zbieranych Pośrednio" musi określać zasady informowania osób, których dane zostały pozyskane pośrednio, o celach, podstawach prawnych, odbiorcach oraz czasie przechowywania danych, zgodnie z przepisami RODO.
    - Dokument powinien zawierać wytyczne dotyczące praw osób, których dane dotyczą, w tym prawa do dostępu, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu oraz cofnięcia zgody na przetwarzanie, a także informacje o zautomatyzowanym podejmowaniu decyzji i profilowaniu.
70. Polityka Ochrony Danych Osobowych
    - Polityka Ochrony Danych Osobowych musi definiować zasady przetwarzania danych osobowych zgodnie z wymaganiami prawnymi, regulacyjnymi i umownymi, a także zapewniać ochronę danych identyfikujących osoby fizyczne poprzez odpowiednie środki techniczne i organizacyjne.
    - Dokument powinien zawierać wytyczne dotyczące zarządzania danymi, w tym prawa osób, których dane dotyczą, przetwarzanie danych wyłącznie przez upoważniony personel oraz wdrażanie zasad „Privacy by design” i „Privacy by default”.
71. Raport z Oceny Skutków Przetwarzania dla Ochrony Danych Osobowych
    - Raport z Oceny Skutków Przetwarzania dla Ochrony Danych Osobowych musi zawierać systematyczny opis przetwarzania danych, celów przetwarzania oraz ocenę proporcjonalności i konieczności w stosunku do tych celów, zgodnie z przepisami RODO.

- Dokument powinien zawierać ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, oraz określenie środków planowanych lub zastosowanych w celu zaradzenia tym ryzykom, wraz z ewentualnymi wnioskami dotyczącymi konieczności konsultacji z organem nadzorczym.

72. Rejestr Czynności Przetwarzania Danych Osobowych
    - Rejestr Czynności Przetwarzania Danych Osobowych musi zawierać szczegółowe informacje o wszystkich czynnościach przetwarzania danych osobowych, w tym cele przetwarzania, kategorie osób, których dane dotyczą, kategorie danych oraz kategorie odbiorców, którym dane są ujawniane.
    - Dokument powinien obejmować opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych w celu ochrony danych osobowych, a także informacje o przekazaniach danych do państw trzecich i planowanych terminach usunięcia danych
73. Rejestr Wszystkich Kategorii czynności Przetwarzania Dokonywanych w Imieniu Administratora
    - Rejestr Wszystkich Kategorii Czynności Przetwarzania Dokonywanych w Imieniu Administratora musi zawierać szczegółowy opis wszystkich kategorii czynności przetwarzania realizowanych przez podmiot przetwarzający na rzecz administratora, w tym dane kontaktowe stron oraz kategorie przetwarzanych danych.
    - Dokument powinien obejmować informacje o przekazaniach danych do państw trzecich, planowane terminy usunięcia danych oraz opis technicznych i organizacyjnych środków bezpieczeństwa wdrożonych w celu ochrony przetwarzanych danych osobowych.
74. Rejestr Zbiorów Danych Osobowych
    - Rejestr Zbiorów Danych Osobowych musi zawierać identyfikację wszystkich zbiorów danych osobowych przetwarzanych przez organizację, w tym ich nazwy, cele przetwarzania oraz czynności przetwarzania realizowane w ramach każdego procesu.
    - Dokument powinien zawierać informacje o administratorze danych, identyfikatory zbiorów oraz procesy związane z przetwarzaniem danych, zapewniając pełną ewidencję przetwarzanych danych osobowych w organizacji.
75. Test Równowagi
    - Test Równowagi musi zawierać ocenę prawnie uzasadnionych interesów realizowanych przez administratora w odniesieniu do interesów, podstawowych praw i wolności osób, których dane dotyczą, w celu ustalenia, czy przetwarzanie danych osobowych na tej podstawie jest zgodne z RODO.
    - Dokument powinien uwzględniać analizę korzyści i ryzyk związanych z przetwarzaniem, w tym ocenę możliwości naruszenia prywatności, anonimowości oraz innych praw osób, których dane dotyczą, aby zdecydować o zastosowaniu prawnie uzasadnionego interesu jako podstawy prawnej przetwarzania.

76. Umowa Przetwarzania Danych Osobowych w Imieniu Administratora
    - Umowa Przetwarzania Danych Osobowych w Imieniu Administratora musi określać zasady przetwarzania danych osobowych przez podmiot przetwarzający, zgodnie z wytycznymi administratora, w tym cel przetwarzania, rodzaje danych oraz kategorie osób, których dane dotyczą.
    - Dokument powinien zawierać wytyczne dotyczące obowiązków obu stron, w tym wymogi dotyczące bezpieczeństwa, obowiązek raportowania naruszeń oraz możliwość audytu zgodności z przepisami o ochronie danych osobowych.
77. Zawiadomienia Osoby, Której Dane Dotyczą o Naruszeniu Ochrony Danych Osobowych
    - Zawiadomienie Osoby, Której Dane Dotyczą, o Naruszeniu Ochrony Danych Osobowych musi informować osobę o charakterze naruszenia, możliwych konsekwencjach dla niej oraz środkach zastosowanych przez administratora w celu zaradzenia skutkom naruszenia, zgodnie z art. 34 RODO.
    - Dokument powinien zawierać szczegółowy opis incydentu, obejmujący datę, czas, okoliczności, kategorie dotkniętych danych oraz zalecenia dla osoby, której dane dotyczą, w celu zminimalizowania negatywnych skutków naruszenia.
78. Wycofanie Zgody na Przetwarzanie Danych Osobowych
    - Dokument "Wycofanie Zgody na Przetwarzanie Danych Osobowych" musi umożliwiać osobom wycofanie zgody na przetwarzanie ich danych osobowych, zgodnie z art. 7 RODO, poprzez złożenie odpowiedniego wniosku zawierającego dane osoby oraz zakres wycofanej zgody.
    - Dokument powinien zawierać sekcje umożliwiające określenie rodzaju danych, których przetwarzanie zostaje wycofane, oraz cele przetwarzania, z których osoba chce wycofać swoją zgodę
79. Zgoda na Przetwarzanie Danych Osobowych
    - Dokument "Zgoda na Przetwarzanie Danych Osobowych" musi umożliwiać osobie wyrażenie dobrowolnej i świadomej zgody na przetwarzanie jej danych osobowych, zgodnie z art. 6 RODO, z wyszczególnieniem rodzajów danych oraz celów ich przetwarzania.
    - Dokument powinien zawierać informację o prawie osoby do wycofania zgody w dowolnym momencie, bez wpływu na zgodność z prawem wcześniejszego przetwarzania, oraz o łatwości wycofania zgody na równi z jej wyrażeniem.