Struktura przedmiotowa

Wybrany element: Przedmiot Audytu

- A.5 POLITYKI BEZPIECZEŃSTWA INFORMACJI
- A.5.1 Kierunki bezpieczeństwa informacji określane przez kierownictwo
- A.5.1.1 Polityki dotyczące bezpieczeństwa informacji
- A.5.1.2 Przegląd polityk bezpieczeństwa informacji

- A.6 ORGANIZACJA BEZPIECZEŃSTWA INFORMACJI
- A.6.1 Organizacja wewnętrzna
- A.6.1.1 Role i odpowiedzialność za bezpieczeństwo informacji
- A.6.1.2 Rozdzielanie obowiązków
- A.6.1.3 Kontakty z organami władzy
- A.6.1.4 Kontakty z grupami zainteresowanych specjalistów
- A.6.1.5 Bezpieczeństwo informacji w zarządzaniu projektami

- A.6.2 Urządzenia mobilne i telepraca.
- A.6.2.1 Polityka stosowania urządzeń mobilnych
- A.6.2.2 Telepraca

- A.7 BEZPIECZEŃSTWO ZASOBÓW LUDZKICH
- A.7.1 Przed zatrudnieniem
- A.7.1.1 Postępowanie sprawdzające
- A.7.1.2 Warunki zatrudnienia

- A.7.2 Podczas zatrudnienia
- A.7.2.1 Odpowiedzialność kierownictwa
- A.7.2.2 Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
- A.7.2.3 Postępowanie dyscyplinarne

- A.7.3 Zakończenie i zmiana zatrudnienia
- A.7.3.1 Zakończenie zatrudnienia lub zmiana zakresu obowiązków

- A.8 ZARZĄDZANIE AKTYWAMI
- A.8.1 Odpowiedzialność za aktywa
- A.8.1.1 Inwentaryzacja aktywów
- A.8.1.2 Własność aktywów
- A.8.1.3 Akceptowalne użycie aktywów
- A.8.1.4 Zwrot aktywów

- A.8.2 Klasyfikacja informacji
- A.8.2.1 Klasyfikowanie informacji
- A.8.2.2 Oznaczanie informacji
- A.8.2.3 Postępowanie z aktywami

- A.8.3 Postępowanie z nośnikami
- A.8.3.1 Zarządzanie nośnikami wymiennymi
- A.8.3.2 Wycofywanie nośników
- A.8.3.3 Przekazywanie nośników

- A.9 KONTROLA DOSTĘPU
- A.9.1 Wymagania biznesowe wobec kontroli dostępu
- A.9.1.1 Polityka kontroli dostępu
- A.9.1.2 Dostęp do sieci i usług sieciowych

- A.9.2 Zarządzanie dostępem użytkowników

- A.9.2.1 Rejestrowanie i wyrejestrowywanie użytkowników
- A.9.2.2 Przydzielanie dostępu użytkownikom
- A.9.2.3 Zarządzanie prawami uprzywilejowanego dostępu
- A.9.2.4 Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników
- A.9.2.5 Przegląd praw dostępu użytkowników
- A.9.2.6 Odbieranie lub dostosowywanie praw dostępu

- A.9.3 Odpowiedzialność użytkowników

- A.9.3.1 Stosowanie poufnych informacji uwierzytelniających

- A.9.4 Kontrola dostępu do systemów i aplikacji

- A.9.4.1 Ograniczanie dostępu do informacji
- A.9.4.2 Procedury bezpiecznego logowania
- A.9.4.3 System zarządzania hasłami
- A.9.4.4 Użycie uprzywilejowanych programów narzędziowych
- A.9.4.5 Kontrola dostępu do kodów źródłowych programów

- A.10 KRYPTOGRAFIA

- A.10.1 Zabezpieczenia kryptograficzne

- A.10.1.1 Polityka stosowania zabezpieczeń kryptograficznych
- A.10.1.2 Zarządzanie kluczami

- A.11 BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

- A.11.1 Obszary bezpieczne

- A.11.1.1 Fizyczna granica obszaru bezpiecznego
- A.11.1.2 Fizyczne zabezpieczenie wejść
- A.11.1.3 Zabezpieczenie biur, pomieszczeń i obiektów
- A.11.1.4 Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi
- A.11.1.5 Praca w obszarach bezpiecznych
- A.11.1.6 Obszary dostaw i załadunku

- A.11.2 Sprzęt

- A.11.2.1 Lokalizacja i ochrona sprzętu
- A.11.2.2 Systemy wspomagające
- A.11.2.3 Bezpieczeństwo okablowania
- A.11.2.4 Konserwacja sprzętu
- A.11.2.5 Wynoszenie aktywów
- A.11.2.6 Bezpieczeństwo sprzętu i aktywów poza siedzibą
- A.11.2.7 Bezpieczne zbywanie lub przekazywanie do ponownego użycia
- A.11.2.8 Pozostawianie sprzętu użytkownika bez opieki
- A.11.2.9 Polityka czystego biurka i czystego ekranu

- A.12 BEZPIECZNA EKSPLOATACJA

- A.12.1 Procedury eksploatacyjne i odpowiedzialność

- A.12.1.1 Dokumentowanie procedur eksploatacyjnych
- A.12.1.2 Zarządzanie zmianami
- 12.1.3 Zarządzanie pojemnością
- 12.1.4 Oddzielanie środowisk rozwojowych, testowych i produkcyjnych

- A.12.2 Ochrona przed szkodliwym oprogramowaniem

- A.12.2.1 Zabezpieczenia przed szkodliwym oprogramowaniem

- A.12.3 Kopie zapasowe

- A.12.3.1 Zapasowe kopie informacji

- A.12.4 Rejestrowanie zdarzeń i monitorowanie

- A.12.4.1 Rejestrowanie zdarzeń

- A.12.4.2 Ochrona informacji w dziennikach zdarzeń
- A.12.4.3 Rejestrowanie działań administratorów i operatorów
- A.12.4.4 Synchronizacja zegarów

- A.12.5 Nadzór nad oprogramowaniem produkcyjnym

- A.12.5.1 Instalacja oprogramowania w systemach produkcyjnych

- A.12.6 Zarządzanie podatnościami technicznymi

- A.12.6.1 Zarządzanie podatnościami technicznymi
- A.12.6.2 Ograniczenia w instalowaniu oprogramowania

- A.12.7 Rozważania dotyczące audytu systemów informacyjnych

- A.12.7.1 Zabezpieczenia audytu systemów informacyjnych

- A.13 BEZPIECZEŃSTWO KOMUNIKACJI

- A.13.1 Zarządzanie bezpieczeństwem sieci

- A.13.1.1 Zabezpieczenia sieci
- A.13.1.2 Bezpieczeństwo usług sieciowych
- A.13.1.3 Rozdzielanie sieci

- A.13.2 Przesyłanie informacji

- A.13.2.1 Polityki i procedury przesyłania informacji
- A.13.2.2 Porozumienia dotyczące przesyłania informacji
- A.13.2.3 Wiadomości elektroniczne
- A.13.2.4 Umowy o zachowaniu poufności lub nieujawnianiu informacji

- A.14 POZYSKIWANIE, ROZWÓJ I UTRZYMANIE SYSTEMÓW

- A.14.1 Wymagania związane z bezpieczeństwem systemów informacyjnych

- A.14.1.1 Analiza i specyfikacja wymagań związanych z bezpieczeństwem informacji
- A.14.1.2 Zabezpieczanie usług aplikacyjnych w sieciach publicznych
- A.14.1.3 Ochrona transakcji usług aplikacyjnych

- A.14.2 Bezpieczeństwo w procesach rozwoju i wsparcia

- A.14.2.1 Polityka bezpieczeństwa prac rozwojowych
- A.14.2.2 Procedury kontroli zmian w systemach
- A.14.2.3 Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej
- A.14.2.4 Ograniczenia dotyczące zmian w pakietach oprogramowania
- A.14.2.5 Zasady projektowania bezpiecznych systemów
- A.14.2.6 Bezpieczne środowisko rozwojowe
- A.14.2.7 Prace rozwojowe zlecane podmiotom zewnętrznym
- A.14.2.8 Testowanie bezpieczeństwa systemów
- A.14.2.9 Testy akceptacyjne systemów

- A.14.3 Dane testowe

- A.14.3.1 Ochrona danych testowych

- A.15 RELACJE Z DOSTAWCAMI

- A.15.1 Bezpieczeństwo informacji w relacjach z dostawcami

- A.15.1.1 Polityka bezpieczeństwa informacji w relacjach z dostawcami
- A.15.1.2 Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami
- A.15.1.3 Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych

- A.15.2 Zarządzanie usługami świadczonymi przez dostawców

- A.15.2.1 Monitorowanie i przegląd usług świadczonych przez dostawców
- A.15.2.2 Zarządzanie zmianami w usługach świadczonych przez dostawców

- A.16 ZARZĄDZANIE INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI

- A.16.1 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz

udoskonaleniami

- A.16.1.1 Odpowiedzialność i procedury
- A.16.1.2 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji
- A.16.1.3 Zgłaszanie słabości związanych z bezpieczeństwem informacji
- A.16.1.4 Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji
- A.16.1.5 Reagowanie na incydenty związane z bezpieczeństwem informacji
- A.16.1.6 Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji
- A.16.1.7 Gromadzenie materiału dowodowego

- A.17 ASPEKTY BEZPIECZEŃSTWA INFORMACJI W ZARZĄDZANIU CIĄGŁOŚCIĄ DZIAŁANIA

- A.17.1 Ciągłość bezpieczeństwa informacji

- A.17.1.1 Planowanie ciągłości bezpieczeństwa informacji
- A.17.1.2 Wdrożenie ciągłości bezpieczeństwa informacji
- A.17.1.3 Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji

- A.17.2 Nadmiarowość

- A.17.2.1 Dostępność środków przetwarzania informacji

- A.18 ZGODNOŚĆ

- A.18.1 Zgodność z wymaganiami prawnymi i umownymi

- A.18.1.1 Określenie stosownych wymagań prawnych i umownych
- A.18.1.2 Prawa własności intelektualnej
- A.18.1.3 Ochrona zapisów
- A.18.1.4 Prywatność i ochrona danych identyfikujących osobę
- A.18.1.5 Regulacje dotyczące zabezpieczeń kryptograficznych

- A.18.2 Przeglądy bezpieczeństwa informacji

- A.18.2.1 Niezależny przegląd bezpieczeństwa informacji
- A.18.2.2 Zgodność z politykami bezpieczeństwa i standardami
- A.18.2.3 Sprawdzanie zgodności technicznej