

KRAJOWE STANDARDY INTEROPERACYJNOŚCI

Systemy informatyczne w administracji publicznej. Wdrażanie i eksploatacja

Spis treści

Nota biograficzna

Wykaz skrótów

1. Akty prawne
2. Inne

Rozdział I. Wprowadzenie do Krajowych Ram Interoperacyjności

Rozdział II. Wymagania w zakresie struktur danych i wymiany danych

1. Formaty danych stosowane w systemach informatycznych
2. Dane w rejestrach publicznych

Rozdział III. Wymagania WCAG

1. Obowiązek tworzenia stron internetowych dostępnych dla osób niepełnosprawnych
2. Wymagania w zakresie postrzegalności
3. Wymagania w zakresie zrozumiałości
4. Wymagania w zakresie kompatybilności

Rozdział IV. Zarządzanie ryzykiem informatycznym

1. Obowiązek wdrożenia procesu zarządzania ryzykiem informatycznym
 - 1.1. Proces zarządzania ryzykiem zgodny z Polską Normą PN-ISO/IEC 27005
 - 1.2. Ryzyko operacyjne a zarządzanie ryzykiem operacyjnym
 - 1.3. Zdefiniowanie zakresu zarządzania ryzykiem na podstawie normy PN-ISO/IEC 27005
2. Identyfikacja i szacowanie ryzyka
 - 2.1. Ocena poziomu ryzyka
 - 2.2. Identyfikacja aktywów informacyjnych
 - 2.2.1. Określenie konsekwencji naruszeń i częstotliwości ich występowania
 - 2.2.2. Sposoby opisywania ryzyka
 - 2.2.3. Inwentaryzacja aktywów informacyjnych i zagrożeń
 - 2.3. Szacowanie konsekwencji naruszenia bezpieczeństwa informacji
 - 2.4. Szacowanie konsekwencji naruszenia bezpieczeństwa aktywów materialnych
 - 2.5. Identyfikacja zagrożeń oraz szacowanie częstotliwości naruszeń bezpieczeństwa spowodowanych przez zagrożenie
3. Postępowanie z ryzykiem
 - 3.1. Poziom ryzyka akceptowalnego
 - 3.2. Osoby odpowiedzialne za podjęcie decyzji dotyczących postępowania z ryzykiem
 - 3.3. Metody postępowania z ryzykiem informatycznym
 - 3.4. Plan postępowania z ryzykiem
4. Monitorowanie poziomu ryzyka
5. Odpowiedzialność za realizację zarządzania ryzykiem –
6. Komunikacja

Rozdział V. Zarządzanie bezpieczeństwem systemów teleinformatycznych

1. System zarządzania bezpieczeństwem informacji
2. Klasyfikacja informacji

3. Zarządzanie dostępem do informacji
 - 3.1. Zasady zarządzania dostępem do informacji
 - 3.2. Zarządzanie uprawnieniami
 - 3.3. Zarządzanie danymi uwierzytelniającymi
 - 3.4. Dostęp do kont administracyjnych
 - 3.5. Odbieranie dostępu do systemów informatycznych
 - 3.6. Modyfikacja uprawnień
 - 3.7. Przegląd uprawnień
 - 3.8. Prawa dostępu w systemach zarządzanych przez podmioty zewnętrzne
 - 3.9. Wymagania w zakresie funkcjonalności systemów informatycznych
4. Użytkowanie systemów informatycznych
 - 4.1. Zasady bezpiecznego korzystania z systemów informatycznych
 - 4.2. Zasady przechowywania danych
 - 4.3. Przekazywanie informacji
 - 4.4. Zasady korzystania przez użytkowników z Internetu
 - 4.5. Bezpieczeństwo sprzętu informatycznego i oprogramowania
5. Inwentaryzacja aktywów informacyjnych
6. Zarządzanie sprzętem i oprogramowaniem
 - 6.1. Zarządzanie sprzętem
 - 6.2. Zarządzanie oprogramowaniem
7. Zarządzanie kopiami zapasowymi
8. Monitorowanie systemów informatycznych i zarządzanie pojemnością
 - 8.1. Zarządzanie logami
 - 8.2. Zarządzanie pojemnością
9. Zarządzanie zmianami i bezpieczeństwo w realizacji projektu
 - 9.1. Proces wprowadzania zmiany
 - 9.2. Bezpieczeństwo informacji podczas realizacji projektu
10. Bezpieczeństwo wymiany danych
11. Ochrona kryptograficzna
 - 11.1. Zadania ochrony kryptograficznej
 - 11.2. System zarządzania certyfikatami
 - 11.3. Wymagania dla algorytmów kryptograficznych i protokołów kryptograficznych
 - 11.4. Ochrona zdalnego dostępu administracyjnego?
12. Ochrona przed złośliwym oprogramowaniem
13. Współpraca z podmiotami zewnętrznymi
14. Zabezpieczenia obszaru przetwarzania informacji
15. Zarządzanie incydentami naruszenia bezpieczeństwa informacji
 - 15.1. Pozyskanie informacji o zdarzeniu, które spowodowało incydent
 - 15.2. Reakcja na incydent
16. Zarządzanie ciągłością informacji
 - 16.1. Zabezpieczenie ciągłości działania
 - 16.2. Plany odtwarzania i zapewnienia ciągłości działania
 - 16.3. Zabezpieczenie ciągłości działania zgodnie z PN-ISO/IEC 24762
17. Procesy zarządzania personelem
18. Dokumentacja zasad zarządzania bezpieczeństwem informacji
 - 18.1. Dokumenty wewnętrzne systemu zarządzania bezpieczeństwem informacji
 - 18.2. Dokumenty zewnętrzne systemu zarządzania bezpieczeństwem informacji
19. Wdrożenie systemu zarządzania bezpieczeństwem informacji
20. Weryfikacja systemu zarządzania bezpieczeństwem informacji

Rozdział VI. Zarządzania usługami realizowanymi przez systemy teleinformatyczne

1. Katalog usług i zarządzanie cyklem życia usług
 - 1.1. Katalog usług

- 1.2. Zarządzanie cyklem życia usług
2. Monitorowanie świadczenia usług
3. Świadczenie usługi przez usługodawcę
 - 3.1. Budżetowanie i rozliczanie kosztów usług
 - 3.2. Współpraca z dostawcami zewnętrznymi
 - 3.3. Zarządzanie pojemnością
 - 3.4. Proces zarządzania konfiguracją
4. Kontakt z użytkownikiem
 - 4.1. Procesy rozwiązywania w normie PN-ISO/IEC 20000-1:2014-01
 - 4.2. Zarządzanie incydentami
 - 4.3. Proces zarządzania problemem
 - 4.4. Proces wnioskowania o usługi
5. Wdrożenie systemu zarządzania usługami
 - 5.1. System zarządzania usługami a system zarządzania bezpieczeństwem informacji
 - 5.2. Procedura zarządzania dokumentami
 - 5.3. Doskonalenie systemu zarządzania usługami
 - 5.4. Plan zarządzania usługami
 - 5.5. Proces zarządzania ryzykiem w ramach zarządzania usługami

Rozdział VII. Wdrożenie Krajowych Ram Interoperacyjności w instytucji

1. Audyt weryfikujący stopień dostosowania instytucji do wymagań określonych w KrajRamIntR
 - 1.1. Audyt infrastruktury informatycznej
 - 1.2. Audyt procesów zarządzania infrastrukturą informatyczną
 - 1.3. Przygotowanie raportu z audytu
2. Plan dostosowania instytucji do wymagań określonych w KrajRamIntR
3. Wdrożenie strategii rozwoju infrastruktury informatycznej

Rozdział VIII. Akty prawne

1. Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych