CHESKLISTA NIS2

(C-zgodność, NC-niezgodność)

LP	Wymagania NIS2 (W kolumnie „Wyniki audytu” wpisz czy posiadasz poniższy dokumenty)	Podstawa prawna NIS2	Zakres jaki powinien opisywać dokument	Wyniki weryfikacji	C/NC
1	Polityka analizy ryzyka	Art. 21 ust. 2 lit. a	• Metodyka szacowania ryzyka • Proces szacowania ryzyka • Postępowanie z ryzykiem		
2	Polityka bezpieczeństwa systemów informatycznych	Art. 21 ust. 2 lit. a	• Fizyczne granice bezpieczeństwa • Zabezpieczanie biur, pomieszczeń i obiektów • Monitorowanie bezpieczeństwa fizycznego • Zabezpieczenia nośników informacji • Zabezpieczenia narzędzi pomocniczych • Bezpieczeństwo okablowania • Bezpieczna utylizacja lub ponowne użycie sprzętu • Urządzenia końcowe użytkownika • Instalacja oprogramowania na systemach operacyjnych • Zarządzanie pojemnością • Zarządzanie konfiguracją • Synchronizacja zegara • Kopia zapasowa informacji • Redundancja urządzeń do przetwarzania informacji		

3	Obsługa incydentów	Art. 21 ust. 2 lit. b	• Planowanie i przygotowanie zarządzania incydentami związanymi z bezpieczeństwem informacji • Ocena i decyzja o zdarzeniach związanych z bezpieczeństwem informacji • Reakcja na incydenty związane z bezpieczeństwem informacji • Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji • Zbieranie dowodów		
4	Ciągłość działania	Art. 21 ust. 2 lit. c	• Bezpieczeństwo informacji podczas zakłóceń • Gotowość ICT do zapewnienia ciągłości biznesowej		
5	Bezpieczeństwo łańcucha dostaw	Par. Art. 21 ust. 2 lit. d	• Bezpieczeństwo informacji w relacjach z dostawcami • Zajmowanie się bezpieczeństwem informacji w ramach umów z dostawcami • Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw ICT • Monitorowanie, przegląd i zarządzanie zmianami usług dostawców • Bezpieczeństwo informacji przy korzystaniu z usług w chmurze		
6	Bezpieczeństwo utrzymywania i rozwoju sieci i systemów informatycznych	Par. Art. 21 ust. 2 lit. e	• Działania monitorujące • Filtrowanie sieci • Bezpieczeństwo sieci • Bezpieczeństwo usług sieciowych • Segregacja sieci • Bezpieczny cykl rozwojowy • Wymagania bezpieczeństwa aplikacji • Bezpieczna architektura systemu i zasady inżynierii • Bezpieczne kodowanie		

			• Testy bezpieczeństwa w fazie rozwoju i akceptacji • Rozwój zlecony na zewnątrz • Separacja środowisk deweloperskich, testowych i produkcyjnych • Zarządzanie zmianami • Informacje testowe • Ochrona systemów informatycznych		
7	Postępowanie z podatnościami	Par. Art. 21 ust. 2 lit. e	• Ochrona przed złośliwym oprogramowaniem • Zarządzanie lukami technicznymi • Zapobieganie wyciekom danych		
8	Polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie	Par. Art. 21 ust. 2 lit. f	• Przegląd systemu zarządzania • Niezależny przegląd bezpieczeństwa informacji • Zgodność z politykami, zasadami i standardami bezpieczeństwa informacji • Audyt wew.		
9	Podstawowe praktyki cyberhigieny (postępowanie z informacjami, czyste biurko, czysty ekran)	Par. Art. 21 ust. 2 lit. g	• Ochrona przed zagrożeniami fizycznymi i środowiskowymi • Praca w bezpiecznych miejscach • Czyste biurko i czysty ekran • Umiejscowienie i ochrona sprzętu • Bezpieczeństwo majątku poza lokalem		
10	Kryptografia i szyfrowania	Par. Art. 21 ust. 2 lit. h	• Bezpieczne uwierzytelnianie • Usuwanie informacji • Maskowanie danych • Logowanie • Wykorzystanie kryptografii		

11	Bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami	Par. Art. 21 ust. 2 lit. i	• Spis informacji i innych powiązanych aktywów • Dopuszczalne wykorzystanie informacji i innych powiązanych aktywów • Dopuszczalne wykorzystanie informacji i innych powiązanych aktywów • Zwrot aktywów • Klasyfikacja informacji • Etykietowanie informacji • Kontrola dostępu • Zarządzanie tożsamością • Informacje uwierzytelniające • Prawa dostępu • Kompetencje • Uświadamiania • Postępowanie sprawdzające przed zatrudnieniem • Warunki zatrudnienia • Postępowanie dyscyplinarne • Obowiązki po rozwiązaniu lub zmianie zatrudnienia • Umowy o zachowaniu poufności lub o zachowaniu poufności • Raportowanie zdarzeń związanych z bezpieczeństwem informacji • Uprzywilejowane prawa dostępu • Ograniczenie dostępu do informacji • Dostęp do kodu źródłowego • Korzystanie z uprzywilejowanych programów narzędziowych		
12	Szkolenia z zakresu cyberbezpieczeństwa	Par. Art. 21 ust. 2 lit. g	•Kompetencje •Świadomość bezpieczeństwa informacji, edukacja i szkolenia		

13	Uwierzytelnianie wieloskładnikowe lub ciągłe zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu	Par. Art. 21 ust. 2 lit. j	• Transfer informacji • Praca zdalna		