Wdrożony System Zarządzania Bezpieczeństwem Informacji w obejmuje swoim zakresem Szpital Wojewódzki im. dr. Ludwika Rydygiera w Suwałkach		
Rozdział	**Opis normy/wymaganie**	**Sposób realizacji**
A.5 Polityka bezpieczeństwa		
Cel: zapewnienie przez kierownictwo wytycznych i wsparcia dla działań na rzecz bezpieczeństwa informacji, zgodnie z wymaganiami biznesowymi oraz właściwymi normami i regulacjami.		
A.5.1 Polityka bezpieczeństwa informacji		
A.5.1.1	Dokument polityki bezpieczeństwa informacji	**SZBI_01_Polityka_bezpieczenstwa_informacji (wraz załącznikami)** została zatwierdzona przez najwyższe kierownictwo oraz ogłoszona wszystkim pracownikom za pośrednictwem wewnętrznego zasobu sieciowego.
A 5.1.2	Przegląd informacji polityki bezpieczeństwa	**SZBI_01_Polityka_bezpieczenstwa_informacji (wraz załącznikami)** została zweryfikowana przez właścicieli aktywów i właścicieli procesów pod kątem jej adekwatności do obecnego stanu faktycznego. Najbliższy przegląd jest przewidziany w I kw. 2023r.
A.6 Organizacja bezpieczeństwa informacji		
Cel: Ustanowić strukturę zarządzania w celu zainicjowania oraz nadzorowania wdrażania i eksploatacji bezpieczeństwa informacji w organizacji.		
A.6.1 Organizacja wewnętrzna		
A.6.1 1	Role i odpowiedzialność za bezpieczeństwo informacji	Role i odpowiedzialność osób za poszczególne obszary funkcjonowania SZBI zostały opisane w **pkt. 7 SZBI_01_Polityka_bezpieczenstwa_informacji**
A.6 1.2	Rozdzielanie obowiązków	Podział obowiązków w zakresie działania SZBI, nadzoru nad SZBI oraz w obszarze decyzyjnym został rozdzielony tak by nie powodować konfliktów w ww. obszarach. **(pkt. 7 SZBI_01_Polityka_bezpieczenstwa_informacji)**
A.6.1.3	Kontakty z organami władzy	Zgodnie z **SZBI-P-9 Powołanie i odwołanie IOD** Inspektor Ochrony Danych podlega zgłoszeniu do Prezesa Urzędu Ochrony Danych Osobowych i pozostaje punktem kontaktowym dla urzędu.
A.6.1.4	Kontakty z grupami zainteresowanych specjalistów	Organizacja utrzymuje stosowne kontakty z grupami zainteresowanych specjalistów oraz innymi specjalistycznymi forami oraz stowarzyszeniami zawodowymi z obszaru bezpieczeństwa informacji.
A.6.1.5	Bezpieczeństwo informacji w zarządzaniu projektami	Zgodnie z procedurą domyślnej ochrony danych osobowych **SZBI-P-6 Domyślna ochrona danych osobowych** przewidziana jest ocena ryzyka dla bezpieczeństwa informacji.
A.6.2 Urządzenia mobilne i telepraca		
Cel: Zapewnić bezpieczeństwo telepracy i stosowania urządzeń mobilnych		
A.6.2.1	Polityka stosowania urządzeń mobilnych	**IT-I-1 Instrukcja korzystania z urządzeń mobilnych**
A.6.2.2	Telepraca	**IT-I-2 Instrukcja pracy zdalnej**
A.7 Bezpieczeństwo zasobów ludzkich		
A.7.1 Przed zatrudnieniem		

Cel: Zapewnić, żeby pracownicy i kontrahenci rozumieli swoją odpowiedzialność i byli odpowiednimi kandydatami do wypełnienia ról, do których są przewidziani.		
A.7.1.1	Postępowanie sprawdzające	HR-I-1 Procedura rekrutacji
A.7.1.2	Warunki zatrudnienia	HR-I-2 Zachowanie poufności
A.7.2 Podczas zatrudnienia		
Cel: Zapewnić, żeby pracownicy i kontrahenci byli świadomi swoich obowiązków dotyczących bezpieczeństwa informacji i wypełniali je.		
A.7.2.1	Odpowiedzialność kierownictwa	Najwyższe kierownictwo zgodnie z ogłoszoną SZBI_01_Polityka_bezpieczenstwa_informacji (pkt. 3) zostało zobowiązane do przestrzegania SZBI. Dodatkowo każda osoba upoważniona do przetwarzania danych osobowych podpisała dodatkowe oświadczenie o zachowaniu poufności SZBI-P-4-W1 Upoważnienie do przetwarzania danych osobowych
A.7.2.2	Uświadomienie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	Cały personel jest objęty szkoleniami wstępnymi oraz okresowymi z ochrony danych osobowych oraz bezpieczeństwa informacji zgodnie z SZBI-P-4 Szkolenie personelu
A.7.2.3	Postępowanie dyscyplinarne	HR-I-3 Odpowiedzialność personelu
A.7.3 Zakończenie i zmiana zatrudnienia		
Cel: Zabezpieczyć interesy organizacji w trakcie procesu zmiany lub zakończenia zatrudnienia.		
A.7.3.1	Zakończenie zatrudnienia lub zmiana zakresu obowiązków	HR-I-4 Procedura obiegowa
A.8 Zarządzanie aktywami		
A.8.1 Odpowiedzialność za aktywa		
Cel: Zidentyfikować aktywa organizacji i zdefiniować właściwą odpowiedzialność w dziedzinie ich ochrony.		
A.8.1.1	Inwentaryzacja aktywów	Inwentaryzacja aktywów jest na bieżąco prowadzona przez właścicieli aktywów zgodnie z SZBI-P-1 Klasyfikacja zasobów informacyjnych
A.8.1.2	Własność aktywów	Aktywa zostały przypisane do procesów za które są odpowiedzialni poszczególni właściciele procesów zgodnie z SZBI-P-1-W1 Wykaz zasobów informacyjnych
A.8.1.3.	Akceptowalne użycie aktywów	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.8.1.4	Zwrot aktywów	HR-I-4 Procedura obiegowa
A.8.2 Klasyfikacja informacji		
Cel: Zapewnić przypisanie informacjom odpowiedniego poziomu ochrony, zgodnego z ich wagą dla organizacji.		
A.8.2.1	Klasyfikowanie informacji	Aktywa informacyjne zostały sklasyfikowane zgodnie z podziałem określonym w SZBI-P-1 Klasyfikacja zasobów informacyjnych oraz przypisano im wartości zgodnie z SZBI-P-2 Analiza ryzyka.
A.8.2.2	Oznaczanie informacji	Procedura oznaczania informacji została określona w SZBI-P-1 Klasyfikacja zasobów informacyjnych (pkt. 4.4) w zakresie oznaczeń „Informacje poufne” lub „Tajemnica przedsiębiorstwa”.
A.8.2.3	Postępowanie z aktywami	Procedura postepowania z aktywami została określona w SZBI-P-1 Klasyfikacja zasobów informacyjnych (pkt. 4.5)

A.8.3 Postępowanie z nośnikami		
Cel: Zapobiec nieuprawnionemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu informacji zapisanych na nośnikach.		
A.8.3.1	Zarządzanie nośnikami wymiennymi	IT-I-1 Instrukcja korzystania z urządzeń mobilnych
A.8.3.2	Wycofanie nośników	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.8.3.3	Przekazywanie nośników	IT-I-1 Instrukcja korzystania z urządzeń mobilnych
A.9 Kontrola dostępu		
A.9.1 Wymagania biznesowe wobec kontroli dostępu		
Cel: Ograniczyć dostęp do informacji i środków przetwarzania informacji.		
A.9.1.1	Polityka kontroli dostępu	ADM-I-1 Procedura kontroli dostępu
A.9.1.2	Dostęp do sieci i usług sieciowych	IT-I-4 Instrukcja przydzielania i odbierania dostępów użytkownikom
A.9.2 Zarządzanie dostępem użytkowników		
Cel: Zapewnić dostęp uprawnionym użytkownikom i zapobiec nieuprawnionemu dostępowi do systemów i usług.		
A.9.2.1	Rejestrowanie i wyrejestrowanie użytkowników	IT-I-4 Instrukcja przydzielania i odbierania dostępów użytkownikom
A.9.2.2	Przydzielanie dostępu użytkownikom	IT-I-4 Instrukcja przydzielania i odbierania dostępów użytkownikom
A.9.2.3	Zarządzanie prawami uprzywilejowanego dostępu	IT-I-5 Instrukcja przydzielania dostępów administracyjnych
A.9.2.4	Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników	IT-I-4 Instrukcja przydzielania i odbierania dostępów użytkownikom
A.9.2.5	Przegląd praw dostępu użytkowników	IT-I-4 Instrukcja przydzielania i odbierania dostępów użytkownikom
A.9.2.6	Odbieranie lub dostosowywanie praw dostępu	IT-I-4 Instrukcja przydzielania i odbierania dostępów użytkownikom
A.9.3 Odpowiedzialność użytkowników		
Cel: Zapewnić rozliczalność użytkowników w celu ochrony ich informacji uwierzytelniających.		
A.9.3.1	Stosowanie poufnych informacji uwierzytelniających	IT-I-6 Polityka haseł
A.9.4 Kontrola dostępu do systemów i aplikacji		
Cel: Zapobiec nieuprawnionemu dostępowi do systemów i aplikacji.		
A.9.4.1	Ograniczenie dostępu do informacji	IT-I-6 Polityka haseł
A.9.4.2	Procedury bezpiecznego logowania	IT-I-6 Polityka haseł
A.9.4.3	System zarządzania hasłami	IT-I-6 Polityka haseł
A.9.4.4	Użycie uprzywilejowanych programów narzędziowych	IT-I-5 Instrukcja przydzielania dostępów administracyjnych
A.9.4.5	Kontrola dostępu do kodów źródłowych programów	IT-I-5 Instrukcja przydzielania dostępów administracyjnych
A.10 Kryptografia		
A.10.1 Zabezpieczenia kryptograficzne		
Cel: Zapewnić właściwe i skuteczne wykorzystanie kryptografii do ochrony poufności, autentyczności i/lub integralności informacji.		

A.10.1.1	Polityka stosowania zabezpieczeń kryptograficznych	IT-I-7 Polityka stosowania zabezpieczeń kryptograficznych
A.10.1.2	Zarządzanie kluczami	IT-I-7 Polityka stosowania zabezpieczeń kryptograficznych
A.11 Bezpieczeństwo fizyczne i środowiskowe		
A.11.1 Obszary bezpieczne		
Cel: Zapobiec nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w informacjach i środkach przetwarzania informacji należących do organizacji.		
A.11.1.1	Fizyczna granica obszaru bezpiecznego	ADM-I-1 Procedura kontroli dostępu
A.11.1.2	Fizyczne zabezpieczenie wejść	ADM-I-1 Procedura kontroli dostępu
A.11.1.3	Zabezpieczenie biur, pomieszczeń i obiektów	ADM-I-1 Procedura kontroli dostępu
A.11.1.4	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	ADM-I-1 Procedura kontroli dostępu oraz Instrukcja BHP.
A.11.1.5	Praca w obszarach bezpiecznych	ADM-I-1 Procedura kontroli dostępu oraz ADM-I-3 Polityka czystego biurka i ekranu
A.11.1.6	Obszary dostaw i załadunku	ADM-I-1 Procedura kontroli dostępu
A.11.2 Sprzęt		
Cel: Zapobiec utracie, uszkodzeniu, kradzieży lub utracie integralności aktywów oraz zakłóceniom w działaniu organizacji.		
A.11.2.1	Lokalizacja i ochrona sprzętu	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.11.2.2	Systemy wspomagające	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.11.2.3	Bezpieczeństwo okablowania	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.11.2.4	Konserwacja sprzętu	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.11.2.5	Wynoszenie aktywów	IT-I-1 Instrukcja korzystania z urządzeń mobilnych
A.11.2.6	Bezpieczeństwo sprzętu i aktywów poza siedzibą	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.11.2.7	Bezpieczne zbywanie lub przekazywanie do ponownego użycia	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.11.2.8	Pozostawianie sprzętu użytkownika bez opieki	IT-I-1 Instrukcja korzystania z urządzeń mobilnych
A.11.2.9	Polityka czystego biurka i czystego ekranu	ADM-I-3 Polityka czystego biurka i ekranu
A.12 Bezpieczna eksploatacja		
A.12.1 Procedury eksploatacyjne i odpowiedzialność		
Cel: Zapewnić poprawną i bezpieczna eksploatację środków przetwarzania informacji.		
A.12.1.1	Dokumentowanie procedur eksploatacyjnych	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.12.1.2	Zarządzanie zmianami	Zgodnie z procedurą domyślnej ochrony danych osobowych SZBI-P-6 Domyślna ochrona danych osobowych przewidziany jest mechanizm nadzoru przez Inspektora Ochrony Danych nad zmianami w procesach.

A.12.1.3	Zarządzanie pojemnością	IT-I-4 Instrukcja przydzielania i odbierania dostępów użytkownikom
A.12.1.4	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	IT-I-4 Instrukcja przydzielania i odbierania dostępów użytkownikom
A.12.2 Ochrona przed szkodliwym oprogramowaniem		
Cel: Zapewnić informacjom i środkom przetwarzania informacji ochronę przez szkodliwym oprogramowaniem.		
A.12.2.1	Zabezpieczenia przed szkodliwym oprogramowaniem	IT-I-8 Oprogramowanie antywirusowe
A.12.3 Kopie zapasowe		
Cel: Chronić przed utratą danych.		
A.12.3.1	Zapasowe kopie informacji	IT-I-9 Polityka kopii zapasowych
A.12.4 Rejestrowanie zdarzeń i monitorowanie		
Cel: Rejestrować zdarzenia i zbierać materiał dowodowy.		
A.12.4.1	Rejestrowanie zdarzeń	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.12.4.2	Ochrona informacji w dziennikach zdarzeń	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.12.4.3	Rejestrowanie działań administratorów i operatorów	IT-I-5 Instrukcja przydzielania dostępów administracyjnych
A.12.4.4	Synchronizacja zegarów	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.12.5 Nadzór nad oprogramowaniem produkcyjnym		
Cel: Zapewnić integralność systemów produkcyjnych.		
A.12.5.1	Instalacja oprogramowania w systemach produkcyjnych	IT-I-4 Instrukcja przydzielania i odbierania dostępów użytkownikom
A.12.6 Zarządzanie podatnościami technicznymi		
Cel: Zapobiec wykorzystaniu podatności technicznych.		
A.12.6.1	Zarządzanie podatnościami technicznymi	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.12.6.2	Ograniczenia w instalowaniu oprogramowania	IT-I-4 Instrukcja przydzielania i odbierania dostępów użytkownikom
A.12.7 Rozważania dotyczące audytu systemów informacyjnych.		
Cel: Zminimalizować wpływ działań audytu na systemy produkcyjne.		
A.12.7.1	Zabezpieczenia audytu systemów informacyjnych	SZBI-P-12 Audyty wewnętrzne
A.13 Bezpieczeństwo komunikacji		
A.13.1 Zarządzanie bezpieczeństwem sieci		
Cel: Zapewnić ochronę informacji w sieciach oraz wspomagających je środkach przetwarzania informacji.		
A.13.1.1	Zabezpieczenia sieci	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.13.1.2	Bezpieczeństwo usług sieciowych	IT-I-4 Instrukcja przydzielania i odbierania dostępów użytkownikom
A.13.1.3	Rozdzielanie sieci	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.13.2 Przesyłanie informacji		
Cel: Utrzymać bezpieczeństwo informacji przesyłanych wewnątrz organizacji i wymienianych z podmiotami zewnętrznymi.		
A.13.2.1	Polityki i procedury przesyłania informacji	IT-I-10 Zasady korzystania z poczty elektronicznej

A.13.2.2	Porozumienia dotyczące przesyłania informacji	IT-I-10 Zasady korzystania z poczty elektronicznej
A.13.2.3	Wiadomości elektroniczne	IT-I-10 Zasady korzystania z poczty elektronicznej
A.13.2.4	Umowy o zachowaniu poufności	Dokument SZBI-P-1 Klasyfikacja zasobów informacyjnych wskazuje sposoby postepowania z informacjami poufnymi i wewnętrznymi w zakresie zachowania ich poufności.
A.14 Pozyskiwanie, rozwój i utrzymanie systemów		
A.14.1 Wymagania związane z bezpieczeństwem systemów informacyjnych		
Cel: Zapewnić, żeby bezpieczeństwo informacji było nieodłączną częścią systemów informacyjnych w całym cyklu życia. Dotyczy to również wymagań wobec systemów informacyjnych dostarczających usług w sieciach publicznych.		
A.14.1.1	Analiza i specyfikacja wymagań bezpieczeństwa informacji	IT-I-11 Minimalne wymagania bezpieczeństwa dla systemów informatycznych
A.14.1.2	Zabezpieczanie usług aplikacyjnych w sieciach publicznych	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.14.1.3	Ochrona transakcji usług aplikacyjnych	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.14.2 Bezpieczeństwo w procesach rozwoju i wsparcia.		
Cel: Zapewnić projektowanie i wdrożenie bezpieczeństwa informacji w ramach cyklu życia systemów informacyjnych.		
A.14.2.1	Polityka bezpieczeństwa prac rozwojowych	Organizacja nie prowadzi żadnych prac rozwojowych nad oprogramowaniem, gdyż korzysta z oprogramowania zewnętrznego.
A.14.2.2	Procedury kontroli zmian w systemach	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.14.2.3	Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.14.2.4	Ograniczenia dotyczące zmian w pakietach oprogramowania	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.14.2.5	Zasady projektowania bezpiecznych systemów	Organizacja nie prowadzi żadnych prac rozwojowych nad oprogramowaniem, gdyż korzysta z oprogramowania zewnętrznego.
A.14.2.6	Bezpieczne środowisko rozwojowe	Organizacja nie prowadzi żadnych prac rozwojowych nad oprogramowaniem, gdyż korzysta z oprogramowania zewnętrznego.
A.14.2.7	Prace rozwojowe zlecane podmiotom zewnętrznym	IT-I-11 Minimalne wymagania bezpieczeństwa dla systemów informatycznych
A.14.2.8	Testowanie bezpieczeństwa systemów	IT-I-11 Minimalne wymagania bezpieczeństwa dla systemów informatycznych
A.14.2.9	Testy akceptacyjne systemów	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.14.3 Dane testowe		
Cel: Zapewnić ochronę danych stosowanych do testów		
A.14.3.1	Ochrona danych testowych	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.15 Relacje z dostawcami		
A.15.1 Bezpieczeństwo informacji w relacjach z dostawcami		

Cel: Zapewnić ochronę aktywów organizacji udostępnionych dostawcom.		
A.15.1.1	Polityka bezpieczeństwa informacji w relacjach z dostawcami	SZBI-P-10 Bezpieczeństwo informacji w relacjach z dostawcami.
A.15.1.2	Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami	SZBI-P-10 Bezpieczeństwo informacji w relacjach z dostawcami.
A.15.1.3	Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych	SZBI-P-10 Bezpieczeństwo informacji w relacjach z dostawcami.
A.15.2 Zarządzanie usługami świadczonymi przez dostawców		
Cel: Utrzymać uzgodniony poziom bezpieczeństwa informacji i świadczonych usług zgodnie z umowami z dostawcami.		
A.15.2.1	Monitorowanie i przegląd usług świadczonych przez dostawców	SZBI-P-10 Bezpieczeństwo informacji w relacjach z dostawcami.
A.15.2.2	Zarządzanie zmianami w usługach świadczonych przez dostawców	SZBI-P-10 Bezpieczeństwo informacji w relacjach z dostawcami.
A.16 Zarządzanie incydentami związanymi z bezpieczeństwem informacji		
A.16.1 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami		
Cel: Zapewnić spójne i skuteczne podejście do zarządzania incydentami związanymi z bezpieczeństwem informacji, z uwzględnieniem informowania o zdarzeniach i słabościach.		
A.16.1.1	Odpowiedzialność i procedury	SZBI-P-11 Zarządzanie naruszeniami ochrony danych osobowych
A.16.1.2	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	SZBI-P-11 Zarządzanie naruszeniami ochrony danych osobowych
A.16.1.3	Zgłaszanie słabości związanych z bezpieczeństwem informacji	SZBI-P-11 Zarządzanie naruszeniami ochrony danych osobowych
A.16.1.4	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji	SZBI-P-11 Zarządzanie naruszeniami ochrony danych osobowych
A.16.1.5	Reagowanie na incydenty związane z bezpieczeństwem informacji	SZBI-P-11 Zarządzanie naruszeniami ochrony danych osobowych
A.16.1.6	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji	SZBI-P-11 Zarządzanie naruszeniami ochrony danych osobowych
A.16.1.7	Gromadzenie materiału dowodowego	SZBI-P-11 Zarządzanie naruszeniami ochrony danych osobowych
A.17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania		
A.17.1 Ciągłość bezpieczeństwa informacji		
Cel: Zaleca się uwzględnienie ciągłości bezpieczeństwa informacji w systemach zażądania ciągłością organizacji.		
A.17.1.1	Planowanie ciągłości bezpieczeństwa informacji	IT-I-9 Polityka kopii zapasowych
A.17.1.2	Wdrożenie ciągłości bezpieczeństwa informacji	IT-I-9 Polityka kopii zapasowych

A.17.1.3	Weryfikowanie przegląd i ocena ciągłości bezpieczeństwa informacji	IT-I-9 Polityka kopii zapasowych
A.17.2 Nadmiarowość		
Cel: Zapewnić dostępność środków przetwarzania informacji		
A.17.2.1	Dostępność środków przetwarzania informacji	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.18 Zgodność		
A.18.1 Zgodność z wymaganiami prawnymi i umownymi		
Cel: Unikać naruszenia zobowiązań prawnych, regulacyjnych lub umownych związanych z bezpieczeństwem informacji oraz innych wymagań dotyczących bezpieczeństwa		
A.18.1.1	Określenie stosownych wymagań prawnych i umownych	SZBI-W-1 Wykaz aktów prawnych i standardów
A.18.1.2	Prawa własności intelektualnej	IT-I-3 Instrukcja eksploatacji sprzętu informatycznego
A.18.1.3	Ochrona zapisów	SZBI-P-1 Klasyfikacja zasobów informacyjnych
A.18.1.4	Prywatność i ochrona danych identyfikujących osobę	SZBI-P-1 Klasyfikacja zasobów informacyjnych
A.18.1.5	Regulacje dotyczące zabezpieczeń kryptograficznych	IT-I-7 Polityka stosowania zabezpieczeń kryptograficznych
A.18.2 Przeglądy bezpieczeństwa informacji		
Cel: Zapewnić zgodne z politykami organizacji i procedurami wdrożenie i stosowanie zasad bezpieczeństwa informacji.		
A.18.2.1	Niezależny przegląd bezpieczeństw informacji	SZBI-P-12 Audyty wewnętrzne
A.18.2.2	Zgodność z politykami bezpieczeństw i standardami	SZBI-P-14 Zarządzanie dokumentacją SZBI
A.18.2.3	Sprawdzanie zgodności technicznej	SZBI-P-12 Audyty wewnętrzne

DYREKTOR
Szpitala Wojewódzkiego
im. dr. Ludwika Rydygiera w Suwałkach

/-/ Adam Szałanda