Deklaracja stosowania

Karta zmian

Nr	Zmiany		Opis zmiany	Data zmiany	Podpis autora
	Rozdział u	Strona nr			

Zatwierdzenia

Zespół	Imię i nazwisko stanowisko	Data	Podpis
Opracował	Krzysztof Janicki	01.06.2017	
Sprawdził	Grzegorz Bula PZJ	01.06.2017	
Sprawdził	Krzysztof Kretek KKO Nit	01.06.2017	

Zatwierdził	Ryszard Rudnik DN	01.06.2017	

1. Obszar wdrożenia systemu zarządzania bezpieczeństwem informacji

System zarządzania bezpieczeństwem informacji zgodny z normą ISO 27001:20013 został wdrożony w Szpitalu Rejonowym im. dr. Józefa Rostka w Raciborzu, przy ul. Gamowskiej 3.
Obszar objęty systemem obejmuje wszystkie budynki Szpitala wraz z całą infrastrukturą.

2. Zakres systemu zarządzania bezpieczeństwem informacji

Zakres Systemu Bezpieczeństwa Informacji określono w Przewodniku ZSZ.

3. Współdzielenie procedur w ZSZ.

W ramach SZBI wykorzystuje się procedury systemowe opracowane dla systemu zarządzania jakością, zgodnie z nowym wzorem struktury norm dotyczących systemów zarządzania.

4. Cele stosowania zabezpieczeń i zabezpieczenia.

Odpowiednie cele stosowania zabezpieczeń oraz zabezpieczenia zostały wybrane i wdrożone tak, aby spełniały wymagania określone przez oszacowanie ryzyka i proces postępowania z ryzykiem.
Wybór jest uzasadniony kryteriami akceptowania ryzyka, jak również wymaganiami prawnymi, regulacyjnymi i wynikającymi z umów.
Cele zabezpieczeń i zabezpieczenia z Załącznika A normy ISO 27001:2013 zostały wybrane jako część procesu szacowania i postępowania z ryzykiem tak, aby odpowiadały określonym wymaganiom.
Wybranie poszczególnych zabezpieczeń podyktowane było zakresem działalności naszego szpitala oraz specyfiką realizacji procesów i doborem infrastruktury.

DEKLARACJA STOSOWANIA

A.5 Polityki bezpieczeństwa informacji				
A.5.1 Prowadzenie zarządu w zakresie bezpieczeństwa informacji			Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie prowadzenia zarządu i wsparcia w zakresie bezpieczeństwa informacji zgodnie z wymaganiami biznesowymi i właściwymi przepisami prawa oraz regulacjami wewnętrznymi.				
A.5.1.1	Polityki bezpieczeństwa informacji	Zabezpieczenie Opracowano zestaw procedur i instrukcji zawierających stosowne ustalenia i wymagania, które zostały zatwierdzone przez najwyższe kierownictwo, opublikowane i podany do wiadomości pracownikom oraz innym stronom zainteresowanym. Zarządzanie dokumentacja uregulowane jest w ramach ZSZ.	Przegląd aktualności dokumentacji przed przeglądem zarządzania.	Dyrektor Pełnomocnik ds. ZSZ
A.5.1.2	Przegląd polityk bezpieczeństwa informacji	Zabezpieczenie Polityki bezpieczeństwa informacji będą poddawane przeglądom przed przeglądem zarządzania albo w razie wystąpienia istotnych zmian celem zapewnienia ich nieprzerwanej przydatności, adekwatności i skuteczności. Zarządzanie dokumentacja uregulowane jest w ramach ZSZ.	Przegląd aktualności dokumentacji przed przeglądem zarządzania oraz po każdej zmianie w Organizacji	Pełnomocnik ds. ZSZ
A.6 Organizacja bezpieczeństwa informacji				
A.6.1 Organizacja wewnętrzna			Sposób monitorowania	Odpowiedzialny
Cel: Ustanowienie ramowych wytycznych dla kierownictwa w zakresie inicjowania oraz kontroli wdrożenia i stosowania bezpieczeństwa informacji w obrębie organizacji.				
A.6.1.1	Stanowiska i zakresy odpowiedzialności	Zabezpieczenie Dla każdego stanowiska określono i zatwierdzono upoważnienia do przetwarzania informacji. Pracownicy przyjęli do wiadomości swoje zakresy upoważnień podpisując się pod nimi. Określono również na piśmie zakresy odpowiedzialności i uprawnień	Audit wewnętrzny, inspekcje ABI, bieżący nadzór prowadzony przez NKP oraz NIT. Dokumentacja kadrowa.	Kierownik każdy w swoim zakresie, ABI , KKO NKP oraz Pełnomocnik ZSZ (audit wewnętrzny)
A.6.1.2	Rozgraniczenie obowiązków	Zabezpieczenie Przed określeniem upoważnień Osoba odpowiedzialna za zatwierdzenie upoważnienia, weryfikuje zaproponowany zakres pod katem potencjalnych incydentów wynikających z wykluczających się nawzajem odpowiedzialności.	Audit wewnętrzny, inspekcje ABI, bieżący nadzór prowadzony przez Dział Kadr oraz Dział Informatyki	Kierownik każdy w swoim zakresie, ABI, KKO NKP oraz Pełnomocnik ZSZ (audit wewnętrzny)

A.6.1.3	Kontakt z władzami	Zabezpieczenie Kontakt z władzami ograniczony jest tylko do zakresu wynikającego z wymagań prawnych dotyczących działalności szpitala oraz bieżących spotkań wynikającymi z zaproszeń. Za kontakty z władzami odpowiedzialny jest Dyrektor Szpitala.	Audit wewnętrzny,	Dyrektor Pełnomocnik ZSZ (audit wewnętrzny)
A.6.1.4	Kontakt z specjalnymi grupami zainteresowania	Zabezpieczenie W ramach współpracy z Organizacjami Certyfikującymi i Konsultingowymi, Szpital komunikuje się w zakresie utrzymania i doskonalenia systemu.	Audit wewnętrzny,	Pełnomocnik ds. ZSZ ABI, KKO NIT
A.6.2 Urządzenia mobilne i praca na odległość			Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie bezpieczeństwa pracy na odległość i używania urządzeń mobilnych.				
A.6.2.1	Polityka dla urządzeń mobilnych	Zabezpieczenie Opracowano regulamin użytkowania urządzeń mobilnych - FZSZ-12.1, który korzystający z urządzenia poza siedzibą Szpitala musi przeczytać i potwierdzić zapoznanie się z jego treścią.	Audit wewnętrzny,	KKO NKP, KKO NDG Pełnomocnik ZSZ (audit wewnętrzny)
A.6.2.2	Praca na odległość	Zabezpieczenie Pracownicy mogą wykonywać pracę na odległość jeżeli wynika to z charakteru ich pracy lub za zgoda Dyrektora Szpitala. Podczas pracy na odległość połączenie z serwerami Szpitala odbywa się przy wykorzystaniu usługi VPN. Dostęp zabezpieczony jest indywidualnym loginem i hasłem	Audit wewnętrzny, Bieżący nadzór NIT	KKO NIT Pełnomocnik ZSZ (audit wewnętrzny)
A.6.1.5	Bezpieczeństwo informacji w zarządzaniu projektami	Zabezpieczenie Zasady bezpieczeństwa informacji są uwzględnione w zarządzaniu projektami, bez względu na typ projektu. Szpital stosuje klauzule poufności w zawieranych umowach z wykonawcami projektów technicznych. W przypadku projektów informatyczny realizowanych siłami własnymi Szpitala, dostęp do dany związanych z projektem mają Pracownicy NIT, dostęp zabezpieczony jest indywidualnymi hasłami. Dane są zgrywane na kopie bezpieczeństwa zgodnie z Standardem akredytacyjnym ZI, NR - ZI -2012, „Zarządzanie Informacją”. W przypadku projektów unijnych należy stosować zasady postępowania zgodne z przepisami określonymi przez poszczególne jednostki finansujące, w ramach projektów Unijnych.	Audit wewnętrzny, Inspekcje ABI Bieżący nadzór Kierownika NIT	ABI oraz Kierownik NIT Pełnomocnik ZSZ (audit wewnętrzny)

A.7 Bezpieczeństwo zasobów ludzkich				
A.7.1 Przed zatrudnieniem			Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie, aby pracownicy i wykonawcy rozumieli swoją odpowiedzialność i byli odpowiedni do zadań, których pełnienie zamierza się im powierzyć.				
A.7.1.1	Postępowanie sprawdzające	Zabezpieczenie Uszczegółowienie wymagań następuje w Ogłoszeniu o konkursie na stanowiska lub przy rekrutacji. Weryfikacje kompetencji przeprowadza Komisja lub Właściwy Kierownik KO na podstawie dokumentów dostarczonych przez kandydata .	Audit wewnętrzny, Dokumentacja kadrowa	KKO NKP Pełnomocnik ZSZ (audit wewnętrzny)
A.7.1.2	Zasady i warunki zatrudnienia	Zabezpieczenie Dla pracowników określono zakresy obowiązków i uprawnień oraz upoważnienia do przetwarzania informacji. Zasady zatrudnienia określono w umowach o prace oraz w umowach cywilno-prawnych. Dla firm prowadzących prace na terenie Szpitala warunki realizacji określone są w umowach, które zawierają klauzule poufności.	Audit wewnętrzny, inspekcje ABI,	Pełnomocnik ZSZ (audit wewnętrzny)
A.7.2 W trakcie trwania zatrudnienia			Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie, aby pracownicy i wykonawcy byli świadomi swoich zakresów odpowiedzialności dotyczących bezpieczeństwa informacji i je spełniali.				
A.7.2.1	Odpowiedzialność kierownictwa	Zabezpieczenie Pracownicy oraz inne osoby przed otrzymaniem upoważnienia do przetwarzania informacji, są zapoznani z wymaganiami w zakresie bezpieczeństwa informacji dotyczącymi zakresu stanowiskowego, wynikającymi z dokumentacji SZBI. Zapoznanie pracowników przyjmowanych do pracy udokumentowane jest w karcie obiegowej, a pracowników już zatrudnionych (w przypadku nowego dokumentu) na liście obecności ze szkolenia. Dla firm obcych warunki współpracy określone są w umowach, które zawierają klauzule poufności.	Audit wewnętrzny, inspekcje ABI, dokumentacja kadrowa	KKO NKP, ABI, Pełnomocnik ZSZ (audit wewnętrzny)
A.7.2.2	Świadomość, wykształcenie i szkolenie	Zabezpieczenie Wymagania określono w Standardzie akredytacyjnym „Zarządzanie Zasobami Ludzkimi (ZZ)" oraz procedurami ZSZ. Pracownicy oraz inne osoby przed otrzymaniem upoważnienia do przetwarzania	Dokumentacja kadrowa Ocena pracownicza	Przełożeni pracowników ocenianych. KKO NKP Pełnomocnik ZSZ (audit

		informacji, są zapoznani z wymaganiami w zakresie bezpieczeństwa informacji. Zapoznanie pracowników przyjmowanych do pracy udokumentowane jest w karcie obiegowej, a pracowników już zatrudnionych (w przypadku nowego dokumentu) na liście obecności ze szkolenia.		wewnętrzny)
A.7.2.3	Proces dyscyplinarny	Zabezpieczenie Zasady określono w Procedurze Postępowanie w przypadku naruszenia zasad bezpieczeństwa Informacji .	Audit wewnętrzny, inspekcje ABI,	Pełnomocnik, ABI. KKO NKP
A.7.3 Zakończenie lub zmiana zatrudnienia			Sposób monitorowania	Odpowiedzialny
Cel: Ochrona interesów organizacji, jako część procesu zmiany lub zakończenia zatrudnienia.				
A.7.3.1	Odpowiedzialność związana z zakończeniem lub zmianą zatrudnienia	Zabezpieczenie Zasady zakończenia lub zmiany zatrudnienia opisane są w Regulaminie Pracy. Stosowane są karty obiegowych zgodnie z regulaminem pracy dla pracowników oraz umów cywilno-prawnych. Pracownik musi potwierdzić w Dziale NIT zdanie zasobów IT oraz zamkniecie swojego konta	Audit wewnętrzny, inspekcje ABI, dokumentacja kadrowa	ABI, KKO NKP, Pełnomocnik ZSZ (audit wewnętrzny)
A.8 Zarządzanie aktywami				
A.8.1 Odpowiedzialność za aktywa			Sposób monitorowania	Odpowiedzialny
Cel: Zidentyfikowanie aktywów organizacji i zdefiniowanie odpowiednich obowiązków dotyczących ich ochrony				
A.8.1.1	Inwentaryzacja aktywów	Zabezpieczenie W naszej firmie przeprowadzono inwentaryzacje zasobów z godnie z ustaleniami zawartymi w Procedurze Inwentaryzacja i Analiza Ryzyka	Audit wewnętrzny, Przegląd aktualności inwentaryzacji przed przeglądem zarządzania	Pełnomocnik ZSZ Właściciele Aktywów
A.8.1.2	Własność aktywów	Zabezpieczenie W arkuszach inwentaryzacyjnych określono właścicieli aktywów	Audit wewnętrzny,	Pełnomocnik ZSZ Właściciele Aktywów
A.8.1.3	Akceptowalne użycie aktywów	Zabezpieczenie W Szpitalu stosowane są Upoważnienie do przetwarzania informacji. Nadawane zgodnie z zakresami odpowiedzialności.	Audit wewnętrzny, inspekcje ABI, dokumentacja kadrowa	ABI, KKO NKP, Pełnomocnik ZSZ (audit wewnętrzny)
A.8.1.4	Zwrot aktywów	Zabezpieczenie	Audit wewnętrzny, inspekcje ABI, dokumentacja kadrowa	ABI, KKO NKP, Pełnomocnik ZSZ (audit wewnętrzny)

		Warunkiem podpisania Karty obiegowej dla pracowników i osób realizujących zadania na podstawie umów cywilno-prawnych, jest zwrot powierzonych aktywów informacyjnych. W przypadku stron zewnętrznych (np. firmy obce), stosuje się w zależności od rodzajów aktywów protokoły zdawczo-odbiorcze.		
A.8.2 Klasyfikacja informacji			Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie, uzyskiwania przez informacje poziomu ochrony odpowiedniego do ich znaczenia dla organizacji.				
A.8.2.1	Klasyfikacja informacji	Zabezpieczenie Zasady klasyfikacji informacji określone są w Procedurze Inwentaryzacja i Analiza Ryzyka załącznik nr. 1	Audit wewnętrzny,	Pełnomocnik ZSZ
A.8.2.2	Oznaczanie informacji	Zabezpieczenie Podczas inwentaryzacji aktywów informacyjnych, w tabelach inwentaryzacyjnych, oznacza się zinwentaryzowane informacje. Miejsca przechowywania informacji (segregatory, teczki, itp.) w wersji papierowej oznaczane są etykietami zgodnie z przyjętymi zasadami. Miejsce powstawania informacji określa Regulamin Organizacyjny.	Audit wewnętrzny,	Pełnomocnik ZSZ
A.8.2.3	Postępowanie z informacjami	Zabezpieczenie Zasady postępowania z informacjami w mapie procesów do ZSZ. Postępowanie z informacją związane z akredytacją opisane jest w standardach akredytacyjnych oraz dokumentacji ZSZ.	Audit wewnętrzny,	Pełnomocnik ZSZ
A.8.3 Obsługa nośników			Sposób monitorowania	Odpowiedzialny
Cel: Zapobieganie nieautoryzowanemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu informacji przechowywanych na nośnikach.				
A.8.3.1	Zarządzanie nośnikami wymiennymi	Zabezpieczenie W Szpitalu wprowadzono blokowanie portów USB w celu uniemożliwienia wykorzystywania prywatnych pamięci mobilnych. Zakazane jest nagrywanie płyt CD i DVD bez zgody ABI, wyjątkiem pracowników u których nagrywanie danych wynika z zakresu obowiązków. Pracownicy nie posiadają służbowych pamięci mobilnych, jeśli zajdzie potrzeba użycia takiego urządzenia, KKO NIT, za zgoda ABI może czasowo odblokować port USB Pracownika. Nośniki wymienne wykorzystywane są przez Dział NIT w celu tworzenia kopii zapasowych.	Audit wewnętrzny,	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny)

A.8.3.2	Likwidacja nośników	Zabezpieczenie Takie nośniki jak dyski twarde, dyski mobilne likwidowane są przez wyspecjalizowaną firmę, na wniosek Działu NIT . Płyty CD i DVD niszczone są w niszczarkach przeznaczonych do tego celu.	Audit wewnętrzny,	KKO NIT, KKO w swoich kom org. Pełnomocnik ZSZ (audit wewnętrzny)
A.8.3.3	Transportowanie nośników fizycznych	Zabezpieczenie Nośniki zawierające informacje są zabezpieczane przed nieautoryzowanym dostępem, niewłaściwym użyciem lub uszkodzeniem podczas transportu. Podczas pracy w terenie, pracownicy przewożą dokumenty w zamykanych teczkach lub zaklejone kopertach. Podczas przewożenia dokumentów przez kierowców, dokumenty są zabezpieczone w kopertach i w teczkach na dokumenty. Sprzęt mobilny zabezpieczany jest zgodnie z Regulaminem korzystania z urządzeń mobilnych.	Audit wewnętrzny,	KKO w swoich kom org. Pełnomocnik ZSZ (audit wewnętrzny
A.9	Kontrola dostępu			
A.9.1	Wymagania biznesowe wobec kontroli dostępu		Sposób monitorowania	Odpowiedzialny
Cel: Ograniczenie dostępu do informacji i urządzeń przetwarzających informacje.				
A.9.1.1	Polityka kontroli dostępu	Zabezpieczenie Zasady dostępu do pomieszczeń reguluje Procedura Nadzoru i Gospodarki Kluczami. Standard ZI reguluje zasady dostępu do zasobów informatycznych.	Audit wewnętrzny,	KKO NDG, NIT, KKO NIT, KKO w swoich komórkach organizacyjnych .Pełnomocnik ZSZ (audit wewnętrzny
A.9.1.2	Dostęp do sieci i usług sieciowych	Zabezpieczenie Konfiguracja stacji roboczych jest określana indywidualnie przez dział NIT zgodnie z zakresem obowiązków na danym stanowisku. Dla gości udostępniona jest sieć wydzielona logicznie zabezpieczona hasłem Zasady nadawania uprawnień określa Standard ZI	Weryfikacja wniosku. Zatwierdzanie	Kierownik NIT ABI
A.9.2	Zarządzanie dostępem użytkowników		Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie autoryzowanego dostępu użytkowników i uniemożliwienie nieautoryzowanego dostępu do systemów i usług.				
A.9.2.1	Rejestracja i wyrejestrowanie użytkowników	Zabezpieczenie Zasady rejestracja i wyrejestrowanie użytkowników określono w - Standard ZI	Weryfikacja wniosku. Zatwierdzanie	KKO NIT ABI (nadawanie uprawnień)

A.9.2.2	Umożliwienie dostępu użytkownikom	Zabezpieczenie Standard ZI reguluje zasady dostępu do zasobów informatycznych. Dla gości udostępniona jest sieć wydzielona logicznie zabezpieczona hasłem.	Weryfikacja wniosku Audit wewnętrzny	KKO NIT, ABI , Pełnomocnik ZSZ (audit wewnętrzny
A.9.2.3	Zarządzanie uprzywilejowanymi prawami dostępu	Zabezpieczenie W firmie użytkownikami uprzywilejowanymi w zakresie dostępu do zbiorów elektronicznych są pracownicy Działu Informatyki, Dyrektor Szpitala. Aktualne hasła administratorów systemów IT zapisywane sa na ukrytej partycja na komputerze Dyrektora Szpitala, zmiana haseł administratorów odbywa się raz na rok	Audit wewnętrzny	KKO NIT, ABI (nadawanie uprawnień) , Pełnomocnik ZSZ (audit wewnętrzny
A.9.2.4	Zarządzanie tajnymi informacjami uwierzytelniającymi użytkowników	Zabezpieczenie Zasady przekazywania hasła użytkownikowi oraz zamiany hasła przez użytkownika zawiera Standard ZI	Audit wewnętrzny,	KKO NIT, ABI , Pełnomocnik ZSZ (audit wewnętrzny
A.9.2.5	Przegląd praw dostępu użytkowników	Zabezpieczenie Właściciele aktywów przeglądają prawa dostępu do aktywów co najmniej raz do roku podczas ponownej analizy ryzyka oraz po istotnych zmianach w inwentaryzacji. Pracownicy NIT weryfikują prawa dostępu w celu identyfikacji potencjalnych przypadków wystąpienia „martwych dusz" w systemie informatycznym, potwierdzenie weryfikacji zapisywane jest w „Dzienniku Administratora.	Przygotowanie informacji na przegląd zarządzania. Audit wewnętrzny	KKO NIT, ABI , Pełnomocnik ZSZ (audit wewnętrzny
A.9.2.6	Odbieranie lub modyfikowanie praw dostępu	Zabezpieczenie Zasady określa Standard ZI, w tym zasady odbierania i modyfikacji praw w momencie zakończenia współpracy lub zmiany zasad lub stanowiska. Podstawą do zamknięcia konta użytkownika i odebrania uprawnień jest karta obiegowa	Weryfikacja wniosku Audit wewnętrzny	KKO NIT, ABI , Pełnomocnik ZSZ (audit wewnętrzny
A.9.3 Odpowiedzialność użytkowników			Sposób monitorowania	Odpowiedzialny
Cel: Uczynienie użytkowników odpowiedzialnymi za zabezpieczenie ich informacji uwierzytelniających.				
A.9.3.1	Korzystanie z niejawnych informacji uwierzytelniających	Zabezpieczenie Zasady określone są w Standardzie ZI oraz w Procedurze Czystego biurka i czystego ekranu.	Audit wewnętrzny,	KKO w swoich komórkach organizacyjnych. Pełnomocnik ZSZ

A.9.4 Kontrola dostępu do systemów i aplikacji			Sposób monitorowania	Odpowiedzialny
Cel: Zapobieganie nieautoryzowanemu dostępowi do systemów i aplikacji.				
A.9.4.1	Ograniczanie dostępu do informacji	Zabezpieczenie Zakres dostępu do informacji określają stosowne upoważnienia, które mogą być rozszerzone na podstawie zatwierdzonych wniosków. Zasady w zakresie dostępu do informacji elektronicznej określa Standard ZI	Weryfikacja wniosku Weryfikacja wniosków	KKO NIT, ABI , Pełnomocnik ZSZ (audit wewnętrzny
A.9.4.2	Procedury bezpiecznego logowania się	Zabezpieczenie Dostęp do systemów i aplikacji jest kontrolowany za pomocą zasad bezpiecznego logowania, w oparciu od indywidualne loginy i hasła użytkownika zgodnie z Standardem ZI	Audit wewnętrzny, Inspekcje ABI	KKO NIT, ABI , Pełnomocnik ZSZ (audit wewnętrzny
A.9.4.3	System zarządzania hasłami	Zabezpieczenie Systemy zarządzania hasłami zapewnia odpowiedni poziom bezpieczeństwa zgodnie z obowiązującymi przepisami prawnymi (Ustawa ODO) stosuje się hasła złożone z ośmiu znaków wykorzystujące wszystkie rodzaje znaków, zmiana następuje co 30 dni.	Audit wewnętrzny, Inspekcja	KKO NIT, ABI , Pełnomocnik ZSZ (audit wewnętrzny
A.9.4.4	Używanie uprzywilejowa-nych programów użytkowych	Zabezpieczenie Prawo do konfiguracji i zarządzania specjalistycznym oprogramowaniem informatycznym w tym programami narzędziowymi, antywirusowymi, itp. mają tylko pracownicy NIT. Rozszerzenie uprawnień może nastąpić za zgodą Dyrektora.	Audit wewnętrzny,	KKO NIT, ABI , Pełnomocnik ZSZ (audit wewnętrzny
A.9.4.5	Kontrola dostępu do kodu źródłowego programu	Kody źródłowe do programów będących własnością Szpitala są przechowywane na serwerze Szpitala, dostęp do nich mają administratorzy przy zastosowaniu indywidualnego loginu i hasła. Kody źródłowe znajdują się na kopiach bezpieczeństwa.	Przegląd infrastruktury informatycznej	KKO NIT
A.10 Kryptografia				
A.10.1 Zabezpieczenia kryptograficzne			Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie prawidłowego i efektywnego używania kryptografii w celu ochrony poufności, autentyczności i/lub integralności informacji.				
A.10.1.1	Polityka korzystania z zabezpieczeń kryptograficznych	Zabezpieczenie Zabezpieczenia kryptograficzne stosowane są w relacjach z NFZ, ZUS, Bankami, Urzędem Wojewódzkim, Ministerstwem Finansów, Urzędem Skarbowym. Stosowane rozwiązania są narzucone przez w/w instytucje. W przypadku poczty elektronicznej wykorzystywany jest protokół SSL, do pracy na odległość stosowana jest technologia VPN.	Audit wewnętrzny	Dyrektor, ABI , Pełnomocnik ZSZ (audit wewnętrzny . KKO NM, NKP, NG.

		W przypadku przenoszenie danych osobowych na dyskach twardych poza teren szpitala (laptopy) wymagane jest szyfrowanie twardych dysków.		
A.10.1.2	Zarządzanie kluczami	Zabezpieczenie W przypadku zastosowania metod kryptograficznych, klucz jest przekazywany użytkownikowi osobiście przez pracownika Dział NIT. Użytkownik jest zobowiązany do ochrony klucza kryptograficznego (niewolno go przekazywać innym osobą bez zgodny Kierownik NIT, zapisany musi być przechowywany w kasie pancernej) W Dziale NIT przechowywana jest kopia klucza na wydzielonej partycji serwera, zabezpieczona hasłem dostępu. Podczas wykonywania kopii bezpieczeństwa zasobów serwerowych, klucze kryptograficzne również znajdują się na wykonanej kopii. Po zakończeniu wykorzystywania klucza Dział NIT usuwa kopie klucza.	Audit wewnętrzny	KKO NIT, ABI , Pełnomocnik ZSZ (audit wewnętrzny
A.11 Bezpieczeństwo fizyczne i środowiskowe				
A.11.1 Obszary bezpieczne			Sposób monitorowania	Odpowiedzialny
Cel: Zapobieganie nieautoryzowanemu fizycznemu dostępowi, uszkodzeniu i zagłuszaniu informacji organizacji i jej środków przetwarzania informacji.				
A.11.1.1	Fizyczna granica obszaru bezpiecznego	Zabezpieczenie Obszar objęty systemem obejmuje wszystkie budynki Szpitala wraz z całą infrastrukturą. Ze względu na specyfikę Szpitala w obiektach gdzie prowadzone jest świadczenie usług zdrowotnych, większości ciągów komunikacyjnych poruszają się osoby trzecie. W obszarach tych granicą obszaru bezpiecznego, są wejścia do gabinetów, biur oraz na poszczególne oddziały i obszary zamknięte dla osób trzech (laboratoria, serwerownie, itp.) Zasady dostęp do obszarów Szpitala określono Procedurze Zabezpieczenie dostępu do budynku i pomieszczeń szpitala	Audit wewnętrzny	KKO NDG, NIT, NTE ,KKO w swoich komórkach organizacyjnych. Pełnomocnik ZSZ (audit wewnętrzny
A.11.1.2	Fizyczne zabezpieczenia wejścia	Zabezpieczenie Drzwi do wszystkich pomieszczeń szpitalnych w których przetwarzane są informacje wyposażone są w drzwi zamykane na klucze patentowe. Wejścia na oddziały szpitalne oraz do pomieszczeń specjalnego przeznaczenia (np. serwerownia) zabezpieczane są drzwiami wyposażonymi w zamki uruchamiane kartami magnetycznymi lub wyposażone	Audit wewnętrzny	KKO NDG, NIT, NTE Pełnomocnik ZSZ (audit wewnętrzny. KKO w swoich komórkach organizacyjnych.

		są w zamki cyfrowe. Zasady bezpieczeństwa w tym zakresie określa Standardu ZI .Zasady zarządzanie kluczami określono w Procedurze Nadzór i gospodarka kluczami. Zasady dostęp do obszarów Szpitala określono Procedurze Zabezpieczenie dostępu do budynku i pomieszczeń szpitala		
A.11.1.3	Zabezpieczenie biur, pomieszczeń i urządzeń	Zabezpieczenie Drzwi do wszystkich pomieszczeń szpitalnych w których przetwarzane są informacje wyposażone są w drzwi zamykane na klucze patentowe. Wejścia na oddziały szpitalne oraz do pomieszczeń specjalnego przeznaczenia (np. serwerownia) zabezpieczane są drzwiami wyposażonymi w zamki uruchamiane kartami magnetycznymi lub wyposażone są w zamki cyfrowe. Prawo dostępu do obszarów zabezpieczonych cyfrowo nadaje Kierownik Działu Technicznego na udokumentowany wniosek Kierownika. Pomieszczenia zabezpieczone są w sposób zgodny z zasadami określonymi w Standardu ZI. Zasady zarządzanie kluczami określono w Procedurze Nadzór i gospodarka kluczami. Zasady dostęp do obszarów Szpitala określono Procedurze Zabezpieczenie dostępu do budynku i pomieszczeń szpitala	Audit wewnętrzny	KKO NDG, NIT, NTE Pełnomocnik ZSZ (audit wewnętrzny. KKO w swoich komórkach organizacyjnych.
A.11.1.4	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	Zabezpieczenie Pomieszczenia zabezpieczone są odpowiednimi zabezpieczeniami fizycznymi zgodnie z zasadami bezpieczeństwa określonymi w standardzie ZI oraz w Procedurze Nadzór i gospodarka kluczami. Powiatowy plan zarządzania kryzysowego określa zasady postępowania w sytuacjach kryzysowych w obszarze Miasta Racibórz. Zasady bezpieczeństwa środowiskowego określono w Standardzie ŚO. W Szpitalu zamontowano kamery wewnętrzne i zewnętrzne oraz dla wybranych pomieszczeń system antywłamaniowy i przeciwpożarowy.	Audit wewnętrzny	KKO NB, Pełnomocnik ZSZ (audit wewnętrzny. KKO w swoich komórkach organizacyjnych.
A.11.1.5	Praca w obszarach bezpiecznych	Zabezpieczenie W obszarach bezpiecznych takich jak np.: serwerownia, laboratorium, itp., mogą przebywać tylko uprawnieni pracownicy. Zasady bezpieczeństwa określają: w Standard ZI oraz w Procedura Nadzór i gospodarka kluczami. Zasady rozpoczęcia i zakończenia pracy określono w Procedurze Czystego Biurka i Czystego Ekranu	Audit wewnętrzny	KKO NDG, Pełnomocnik ZSZ (audit wewnętrzny. KKO w swoich komórkach organizacyjnych.
A.11.1.6	Obszary dostaw i załadunku	Zabezpieczenie Obszar dostaw jest to obszar w którym poruszają się pacjenci i ich rodziny oraz inne osoby nie związane z działalnością szpitala oraz miejsca w biurach, gabinetach i na oddziałach, gdzie w/w osoby mogą czasowo przebywać pod nadzorem pracowników szpitala.	Audit wewnętrzny	KKO NDG, NIT, NTE Pełnomocnik ZSZ (audit wewnętrzny.

		Zgodnie z przyjętymi zasadami, osoby trzecie nie mogą mieć dostępu do zasobów informacyjnych podczas czasowego przebywania w obszarze biur, gabinetów i oddziałów. W Szpitalu zamontowano kamery wewnętrzne i zewnętrzne oraz sieć czujek ruchu. Pracownicy opuszczając biura zobowiązani są zamykać pomieszczenia na klucz. Zasady bezpieczeństwa określają: Standard ZI, Procedura Nadzór i gospodarka kluczami, Procedura czystego biurka i ekranu oraz Procedura zabezpieczenie dostępu do budynku i pomieszczeń szpitala.		KKO w swoich komórkach organizacyjnych.
A.11.2 Sprzęt			Sposób monitorowania	Odpowiedzialny
Cel: Zapobieganie utracie, uszkodzeniu, kradzieży lub naruszeniu aktywów oraz przerwaniu działalności organizacji.				
A.11.2.1	Rozmieszczenie i ochrona sprzętu	Zabezpieczenie W Szpitalu stosuje się instalacje elektryczna dedykowaną dla urządzeń infrastruktury informatycznej (czerwone)oraz sprzętu medycznego (zielone). Nadzór nad infrastrukturą budowlaną zapewnia bezpieczeństwo w zakresie zagrożeń naturalnych. Infrastruktura do przetwarzania informacji rozmieszczona jest tylko w obszarze bezpiecznym. Na terenie Szpitala funkcjonuje całodobowa ochrona realizowana przez firmę ochrony mienia. Zasady zarządzania infrastrukturą określa Standard ŚO	Przeglądy budowlane, instalacji, infrastruktury pomocniczej Przeglądy informatyczne (Dziennik administratora)	KKO NDG, NIT, NTE Pełnomocnik ZSZ (audit wewnętrzny. KKO w swoich komórkach organizacyjnych.
A.11.2.2	Systemy wspomagające	Zabezpieczenie W serwerowni zastosowano klimatyzator. Do zasilania infrastruktury IT zastosowano dedykowaną sieć elektryczną. Instalacja czujek p-poż. posiada zasilanie awaryjne celem podtrzymania działania w sytuacji zaniku zasilania zewnętrznego.	Przeglądy budowlane, instalacji, infrastruktury pomocniczej Przeglądy informatyczne, naprawy, serwisy (Raport z przeglądu, Dziennik administratora)	KKO NDG, NIT, NTE , NPp, Pełnomocnik ZSZ (audit wewnętrzny.
A.11.2.3	Bezpieczeństwo okablowania	Zabezpieczenie Okablowanie zasilające i telekomunikacyjne służące do przesyłania danych lub wspomagające usługi informacyjne znajduje się w wewnątrz budynku albo jest zakopane w ziemi. Prowadząc okablowanie teleinformatyczne oddziela się je od instalacji elektrycznej i wodnej stosując oddzielne korytka lub korytka z przegrodą.	Przeglądy budowlane, instalacji, infrastruktury pomocniczej Przeglądy informatyczne (Dziennik administratora)	KKO , NIT, NTE Pełnomocnik ZSZ (audit wewnętrzny.
A.11.2.4	Konserwacja sprzętu	Zabezpieczenie Przeglądy infrastruktury pomocniczej realizowane są przez odpowiedzialne Komórki organizacyjne zgodnie z dokumentacja techniczną lub jeśli taka nie istnieje to w	Przeglądy budowlane, instalacji, infrastruktury pomocniczej	KKO , NIT, NTE Pełnomocnik ZSZ (audit wewnętrzny.

		zaplanowanych odstępach czasu zgodnie z zasadami przyjętymi w ramach systemu zarządzania jakością. Przeglądy infrastruktury informatycznej (serwerownia i infrastruktura teleinformatyczna) prowadzone są co najmniej raz w roku.	Przeglądy infrastruktury informatycznej (Raport)	
A.11.2.5	Wynoszenie aktywów	Zabezpieczenie Wyposażenie do przetwarzania informacji, dokumenty lub oprogramowanie nie mogą być wynoszone poza teren Szpitala bez uprzedniego pisemnego upoważnienia lub formalnego przydziału w ramach zajmowanego stanowiska pracy lub powierzonej funkcji (dokumentacja medyczna, laptopy, smartfony, aparaty fotograficzne itp.).	Audit wewnętrzny	Dyrektor, KKO , NIT, NM Pełnomocnik ZSZ (audit wewnętrzny.
A.11.2.6	Bezpieczeństwo sprzętu i aktywów poza terenem organizacji	Zabezpieczenie Zasady bezpieczeństwa sprzętu informatycznego opisano w Regulamin korzystania ze sprzętu mobilnego. Dokumentacja przenoszona jest w zamykanych teczkach lub kopertach.	Audit wewnętrzny	KKO , NIT, NM Pełnomocnik ZSZ (audit wewnętrzny.
A.11.2.7	Bezpieczna likwidacja sprzętu lub przywró-cenie go do użytku	Zabezpieczenie Sprzęt przetwarzający informacje likwidowany jest przez wyspecjalizowana firmę po uprzednim usunięciu nośników danych.	Audit wewnętrzny	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny.
A.11.2.8	Sprzęt użytkownika bez dozoru	Zabezpieczenie Zabronione jest pozostawiania sprzętu mobilnego bez dozoru. Zasady bezpieczeństwa sprzętu informatycznego opisano w Regulamin korzystania ze sprzętu mobilnego.	Audit wewnętrzny	Pełnomocnik ZSZ (audit wewnętrzny. KKO w swoich komórkach organizacyjnych.
A.11.2.9	Polityka czystego biurka i czystego ekranu	Zabezpieczenie Zasady opisano w Procedurze Czystego Biurka i Czystego Ekranu.	Audit wewnętrzny	Pełnomocnik ZSZ (audit wewnętrzny. KKO w swoich komórkach organizacyjnych.
A.12 Bezpieczeństwo eksploatacji				
A.12.1 Procedury eksploatacyjne i zakresy odpowiedzialności			Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie prawidłowej i bezpiecznej eksploatacji środków przetwarzania informacji.				
A.12.1.1	Udokumentowane procedury eksploatacyjne	Zabezpieczenie Szpital określił niezbędne zasady eksploatacyjne w udokumentowanych standardach, procedurach i instrukcjach	Przegląd aktualności dokumentacji	KKO w swoich komórkach organizacyjnych
A.12.1.2	Zarządzanie zmianami	Zabezpieczenie	Audit wewnętrzny	Pełnomocnik ZSZ, KKO w

		Kierownicy KO, Właściciele Aktywów i ryzyk są zobowiązani do informowania Pełnomocnika o wszelkich zmiana w procesach biznesowych, infrastrukturze oraz przepisach prawa mających wpływ na bezpieczeństwo informacji. Zmiany planowane i wynikające z bieżących potrzeb, oceniane są pod kątem ryzyka związanego z bezpieczeństwem informacji. Efektem analizy może być aktualizacja do Planu postępowania z ryzykiem.	Przegląd zarządzania	swoich komórkach organizacyjnych
A.12.1.3	Zarządzanie pojemnością	Zabezpieczenie Kierownik NIT jest odpowiedzialny za zapewnienie bezawaryjne funkcjonowania systemu informatycznego. W ramach swoich obowiązków na bieżąco monitoruje rezerwy pojemności dysków serwerowych. W sytuacji grożącej awarią, inicjuje działania związane z usuwaniem z dysków zbędnych aktywów oraz może wnioskować do Dyrekcji szpitala o zakup dodatkowych pojemności.	Przeglądu infrastruktury informatycznej, bieżące monitorowanie.	KKO NIT
A.12.1.4	Oddzielanie środowisk rozwojowych, testowych i eksploatacyjnych	Zabezpieczenie Oddzielanie środowisk rozwojowych, testowych i produkcyjnych celem redukcji ryzyk związanych z nieuprawnionym dostępem lub zmianami w środowisku produkcyjnym, odbywa się przy wykorzystaniu środowiska wirtualnego, wydzielonego z zachowaniem zasad bezpieczeństwa, na serwerach roboczych.	Audit wewnętrzny	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny.
A.12.2 Ochrona przed z**łoś**liwym oprogramowaniem			Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie ochrony informacji i środków przetwarzania informacji przed złośliwym oprogramowaniem.				
A.12.2.1	Zabezpieczenia przed złośliwym oprogramowaniem	Zabezpieczenie W celu ochrony serwerów i stacji roboczych stosuje się oprogramowanie antywirusowe ESET endpoint oraz firewall sprzętowy. Pracownik NIT przegląda dzienniki logów w celu zidentyfikowania potencjalnych incydentów.	Audit wewnętrzny Przeglądu infrastruktury informatycznej, w tym przegląd dziennika logów	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny .
A.12.3 Kopie zapasowe			Sposób monitorowania	Odpowiedzialny
Cel: Ochrona przed utratą danych.				
A.12.3.1	Zapasowe kopie informacji	Zabezpieczenie Zasady tworzenia, przechowywania i weryfikacji kopii zapasowych reguluje Standard ZI.	Audit wewnętrzny. Przeglądu inf.. informatycznej	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny

A.12.4 Rejestrowanie i monitorowanie			Sposób monitorowania	Odpowiedzialny
Cel: Rejestrowanie zdarzeń i generowanie dowodów.				
A.12.4.1	Rejestrowanie zdarzeń	Zabezpieczenie Kierownik NIT odpowiada za prowadzenie dziennika administratora, w którym zapisuje się istotne zdarzenia w systemie informatycznym oraz prace serwisowe. Pełnomocnik jest odpowiedzialny za prowadzenie rejestru incydentów. Zdarzenia zachodzące podczas pracy systemu są rejestrowane automatycznie w dziennikach systemowych, które są regularnie przeglądane przez pracowników NIT. Zauważone istotne zdarzenia związane z bezpieczeństwem informacji, rejestrowane są w Dzienniku Administratora, a informacje o nich przekazywane są Pełnomocnikowi, który rejestruje je w Rejestrze Incydentów.	Audit wewnętrzny Przeglądy dzienników logów	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny .
A.12.4.2	Ochrona informacji w dziennikach	Zabezpieczenie Dostęp do dzienników systemowych mają tylko pracownicy Wydziału Informatyki, dostęp jest zabezpieczony hasłem uwierzytelniającym.	Audit wewnętrzny	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny .
A.12.4.3	Dzienniki administratora i operatora	Zabezpieczenie Kierownik NIT odpowiada za prowadzenie dziennika administratora, w którym zapisuje się istotne zdarzenia w systemie informatycznym oraz prace serwisowe. Pełnomocnik jest odpowiedzialny za prowadzenie rejestru incydentów.	Audit wewnętrzny	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny .
A.12.4.4	Synchronizacja zegarów	Zabezpieczenie Synchronizację zegarów urządzeń informatycznych zapewnia się przez stosowanie odpowiednich rozwiązań technicznych wykorzystujących NTP server	Przeglądu infrastruktury informatycznej	KKO NIT
A.12.5 Nadzorowanie oprogramowania eksploatacyjnego			Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie integralności systemów eksploatacyjnych.				
A.12.5.1	Instalacja oprogramo-wania w systemach eksploatacyjnych	Zabezpieczenie Zgodnie z Standardem ZI, instalacje oprogramowania wykonują tylko pracownicy NIT. Pracownicy KO nie posiadają uprawnień Administratora. Po instalacji oprogramowania sprawdzana jest integralność systemu.	Audit wewnętrzny Przeglądu infrastruktury informatycznej	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny).

A.12.6 Zarządzanie podatnością techniczną			Sposób monitorowania	Odpowiedzialny
Cel: Uniemożliwianie wykorzystania podatności technicznych.				
A.12.6.1	Zarządzanie podatnościami technicznymi	Zabezpieczenie Informacje o podatnościach technicznych eksploatowanych systemów i urządzeń technicznych pozyskuje się z prasy fachowej, specjalistycznych portali internetowych, biuletynów. Po uzyskaniu informacji o nowej podatności przeprowadza się stosowne działania oraz jeśli jest taka potrzeba, ponowna ocena ryzyka w obszarze wystąpienia podatności.	Audit wewnętrzny Przeglądu infrastruktury informatycznej	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny).
A.12.6.2	Ograniczenia dotyczące instalacji oprogramo-wania	Zabezpieczenie Zgodnie z Standardem ZI, instalacje oprogramowania wykonują tylko pracownicy Wydziału Informatyki. Instalowane są tylko te programy, które są niezbędne do realizacji procesów Szpitala. Decyzję o doinstalowaniu oprogramowania na wniosek pracowników szpitala podejmuje Kierownik NIT	Audit wewnętrzny	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny).
A.12.7 Uwarunkowania audytów systemów informacyjnych			Sposób monitorowania	Odpowiedzialny
Cel: Zminimalizowanie wpływu czynności audytowych na systemach eksploatacyjnych.				
A.12.7.1	Zabezpieczenia audytowe systemów informacyjnych	Zabezpieczenie Przeglądy systemu informatycznego oraz ewentualne audyty realizowane są po zakończeniu pracy Szpitala. W innym przypadku metodologia audytu jest wcześniej ustalana w taki sposób aby nie zakłócić pracy Szpitala.	Audit wewnętrzny Sprawdzenie metodologii auditu przed jego wykonaniem	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny).
A.13 Bezpieczeństwo wymiany informacji			Sposób monitorowania	Odpowiedzialny
A.13.1 Zarządzanie bezpieczeństwem sieci				
Cel: Zapewnienie ochrony informacji w sieciach oraz używanych w nich pomocniczych środkach przetwarzania informacji.				
A.13.1.1	Zabezpieczenia sieciowe	Zabezpieczenie W punkcie styku z siecią publiczną stosuje się urządzenia wykorzystujące Firewall Cisco ASA . Zasady w zakresie dostępu do sieci teleinformatycznych reguluje Standard ZI	Audit wewnętrzny Przeglądu infrastruktury informatycznej, w tym przegląd dziennika logów	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny).

A.13.1.2	Bezpieczeństwo usług sieciowych	Zabezpieczenie Umowy dotyczące usług sieciowych zawierają wyspecyfikowane wymagania w zakresie bezpieczeństwa informacji. Każdorazowo przez podpisaniem umowy, dział NIT analizuje warunki umowy.	Audit wewnętrzny Przeglądu infrastruktury informatycznej, w tym przegląd dziennika logów	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny).
A.13.1.3	Oddzielanie w sieciach	Zabezpieczenie W Szpitalu wyodrębniono logicznie sieć IT dla Gości. Osoby zewnątrz chcąc skorzystać z połączenia internetowego, otrzymują informacje o zasadach korzystania z wydzielonej sieci.	Audit wewnętrzny Przeglądu infrastruktury informatycznej, w tym przegląd dziennika logów	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny).
A.13.2 Przesyłanie informacji			Sposób monitorowania	Odpowiedzialny
Cel: Utrzymanie bezpieczeństwa informacji przesyłanej w obrębie organizacji i z dowolnym podmiotem zewnętrznym.				
A.13.2.1	Polityki i procedury przesyłania informacji	Zabezpieczenie Przesyłanie informacji podczas pracy na odległość zabezpieczone jest technologią VPN. W komunikacji elektronicznej stosuje się protokół SSL. Przy przesyłaniu danych osobowych poczta elektroniczna stosuje się metody kryptograficzne (np. podpis elektroniczny). Zasady organizacyjne w zakresie przesyłania informacji uregulowano w Standardzie ZI	Audit wewnętrzny Przeglądu infrastruktury informatycznej, w tym przegląd dziennika logów	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny).
A.13.2.2	Umowy o przesyłaniu informacji	Zabezpieczenie Zasady, sposób i zakres przesyłania informacji w Szpitalu wynika z wymagań prawnych odnoszących się do komunikacji z rejestrami publicznymi (Rozporządzenie o krajowych ramach interoperacyjności) oraz umów z Bankami.	Audit wewnętrzny	Dyrektor, KKO NG, NIT, Pełnomocnik ZSZ (audit wewnętrzny).
A.13.2.3	System poczty elektronicznej	Zabezpieczenie Szpital korzysta z zewnętrznego serwera poczty elektronicznej. W komunikacji elektronicznej stosuje się protokół SSL. Przy przesyłaniu danych osobowych poczta elektroniczna stosuje się metody kryptograficzne (np. podpis elektroniczny). Zasady organizacyjne w zakresie przesyłania informacji uregulowano w Standardzie ZI	Audit wewnętrzny Przeglądu infrastruktury informatycznej, w tym przegląd dziennika logów	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny
A.13.2.4	Umowy o poufności lub nie ujawnianiu informacji	Zabezpieczenie W umowach ze stronami zewnętrznymi stosowane są odpowiednie klauzule poufności. W indywidualnych przypadkach na wniosek KKO, klauzule w umowach mogą być zaostrzone.	Audit wewnętrzny	Pełnomocnik ZSZ (audit wewnętrzny. KKO w swoich komórkach organizacyjnych.

A.14 Pozyskiwanie, rozwój i utrzymanie systemów				
A.14.1 Wymagania bezpieczeństwa systemów informacyjnych			Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie, że bezpieczeństwo informacji jest integralną częścią systemów informacyjnych przez cały okres ich życia. Obejmuje to także wymagania względem systemów informacyjnych realizujących usługi za pośrednictwem sieci publicznych.				
A.14.1.1	Analiza i specyfikacja wymagań bezpieczeństwa informacji	Zabezpieczenie Minimalne wymagania dla nowych systemów informacyjnych określa się każdorazowo przed zakupem lub modernizacją w specyfikacji warunków zakupu na podstawie przyjętych regulacji w obszarze zabezpieczeń.	Audit wewnętrzny	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny
A.14.1.2	Zabezpieczanie usług aplikacyjnych w sieciach publicznych	Zabezpieczenie Zasady zabezpieczania usług w sieci publicznej określone są przez Urzędy i Podmioty udostępniające swoje aplikacje szpitalowi w celu komunikacji i raportowania, np.: NFZ, ZUS, Banki itp. Komunikacji z Raciborskim Centrum Medycznym (program eKontrachent) prowadzona jest w protokole bezpiecznym (HTTPS).	Audit wewnętrzny Przeglądu infrastruktury informatycznej, w tym przegląd dziennika logów	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny
A.14.1.3	Ochrona transakcji w ramach usług aplikacyjnych	Zabezpieczenie W celu zapewnienia ochrony transakcji po stronie Szpitala, stosuje się zabezpieczenie antywirusowe i Firewall oraz rozwiązania techniczne w celu uniknięcia przerwania transmisji w wyniku zaniku zasilania w energie elektryczną. Komunikacja realizowana jest przy wykorzystaniu technologii VPN oraz Protokołów bezpiecznych (np. SSL) Wykorzystuje się firewall Cisco ASA.	Audit wewnętrzny Przeglądu infrastruktury informatycznej, w tym przegląd dziennika logów	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny
A.14.2 Bezpieczeństwo w procesach rozwojowych i wsparcia			Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie że bezpieczeństwo informacji jest projektowane i wdrażane w rozwojowym cyklu życia systemów informacyjnych.				
A.14.2.1	Polityka bezpiecznego rozwoju	Zabezpieczenie Prac rozwojowe dotyczące oprogramowania autorskiego prowadzone są według potrzeb Szpitala na polecenie Dyrektora lub z inicjatywy NIT. Programy operacyjne są aktualizowane na bieżąco. W razie potrzeby opracowanie oprogramowania może być zlecone na zewnątrz.	Audit wewnętrzny	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny

A.14.2.2	Procedury nadzorowania zmian w systemach	Zabezpieczenie Nowe oprogramowanie oraz uaktualnienia do oprogramowania są przed zainstalowaniem testowane w środowisku bezpiecznym. Po zainstalowaniu w środowisku produkcyjnym Kierownik NIT monitoruje na bieżąco system operacyjny w celu uchwycenia ewentualnych nieprawidłowości.	Audit wewnętrzny Przeglądu infrastruktury informatycznej, w tym przegląd dziennika logów	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny)
A.14.2.3	Przegląd techniczny aplikacji po zmianach platformy operacyjnej	Zabezpieczenie Po zmianach platformy operacyjnej Kierownik NIT dokonuje przeglądu aplikacji o krytycznym znaczeniu dla działalności Szpitala i przeprowadza testy dla zapewnienia, że nie ma to negatywnego wpływu na działalność organizacji czy bezpieczeństwo informacji	Audit wewnętrzny Przeglądu infrastruktury informatycznej, w tym przegląd dziennika logów	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny)
A.14.2.4	Ograniczenia zmian w pakietach oprogramowania	Zabezpieczenie Bieżące zmiany związane z uaktualnieniami mogą być wprowadzane tylko z zgodą Kierownika NIT. Całkowita zmiana oprogramowania związana z zakupem wymaga zgody Dyrektora Szpitala.	Audit wewnętrzny	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny)
A.14.2.5	Zasady projektowania bezpiecznych systemów	Zabezpieczenie Prac rozwojowe dotyczące oprogramowania autorskiego prowadzone są według potrzeb Szpitala na polecenie Dyrektora lub z inicjatywy NIT. Dział NIT w porozumieniu z KKO przed rozpoczęciem prac rozwojowych, określa dane wejściowe i wyjściowe zawierające wymagane funkcjonalności, wymagania techniczne i organizacyjne oraz jeśli jest taka potrzeba, wymagania prawne. Po zakończeniu prac nad oprogramowaniem, weryfikowane są wyniki prac na zgodność z przyjętymi założeniami. W razie potrzeby opracowanie oprogramowania może być zlecone na zewnątrz. Wymagania określane są w specyfikacji będącej częścią umowy z wykonawcą.	Audit wewnętrzny	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny)
A.14.2.6	Bezpieczne środowisko rozwojowe	Zabezpieczenie Środowisko rozwojowe celem redukcji ryzyk związanych z nieuprawnionym dostępem lub zmianami w środowisku produkcyjnym, odbywa się przy wykorzystaniu środowiska wirtualnego, wydzielonego z zachowaniem zasad bezpieczeństwa, na serwerach roboczych. Dostęp mają tylko pracownicy NIT realizujący projekt.	Audit wewnętrzny	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny)

A.14.2.7	Rozwój w outsourcingu	Zabezpieczenie W razie potrzeby opracowanie oprogramowania może być zlecone na zewnątrz. Wymagania określane są w specyfikacji będącej częścią umowy z wykonawcą. Po zakończeniu prac prowadzone są testy odbiorowe, zakończone spisaniem protokołu odbioru prac.	Audit wewnętrzny	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny)
A.14.2.8	Testowanie bezpieczeństwa systemu	Zabezpieczenie W czasie prac rozwojowych, na ile jest to możliwe prowadzi się testy bezpieczeństwa mające na celu ujawnienie zagrożeń , które mogą wynikać z nowego oprogramowania. W przypadku stwierdzenia ryzyk awarii należ uwzględnić wyniki testów w pracach nad oprogramowaniem i podjąć odpowiednie kroki w celu wyeliminowania przyczyny ryzyka.	Audit wewnętrzny Weryfikacja w trakcie procedur testowych (informacja w dzienniku administratora)	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny)
A.14.2.9	Testowanie odbiorowe systemu	Zabezpieczenie Każdorazowo dla nowych systemów informacyjnych, będących efektem prac rozwojowych ustanawia się zasady testowania w środowisku bezpiecznym, w celu oceny skuteczności prac i realizacji założeń projektowych.	Audit wewnętrzny Weryfikacja w trakcie procedur testowych (protokół odbiorowy)	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny)
A.14.3 Dane testowe			Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie ochrony danych użytych do testowania.				
A.14.3.1	Ochrona danych testowych	Zabezpieczenie Dane testowe chronione są hasłem uwierzytelniającym. Dostęp do nich mają pracownicy NIT. W ramach tworzenia kopii zapasowych dane testowe są również kopiowane.	Audit wewnętrzny Przeglądu infrastruktury informatycznej	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny)
A.15 Relacje z dostawcami				
A.15.1 Bezpieczeństwo informacji w relacjach z dostawcami			Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie ochrony aktywów organizacji do których mają dostęp dostawcy.				
A.15.1.1	Polityka bezpieczeństwa informacji dla relacji z dostawcami	Zabezpieczenie Zasady określające relacje Szpitala z dostawcami określają wymagania prawne. Szpital wyłania dostawców najczęściej poprzez postępowania przetargowe lub wybór ofert.	Audit wewnętrzny, kontrole prowadzone przez organy zwierzchnie	Dyrektor, NG, Pełnomocnik ZSZ (audit wewnętrzny). KKO NZP, DLA, DLM, NTE, NIT, DA,

		Stosowne uregulowania są w dokumentacji przetargowej oraz w umowach z dostawcami. Umowy z dostawcami zawierają klauzule poufności.		DCS, NM, NDG, NKP, NM, NE.
A.15.1.2	Odniesienie do bezpieczeństwa w umowach z dostawcami	Zabezpieczenie Zasady określające relacje Szpitala z dostawcami określają wymagania prawne. Szpital wyłania dostawców najczęściej poprzez postępowania przetargowe lub wybór ofert. Stosowne uregulowania są w dokumentacji przetargowej oraz w umowach z dostawcami. Umowy z dostawcami zawierają klauzule poufności.	Audit wewnętrzny, kontrole prowadzone przez organy zwierzchnie	Dyrektor, NG, Pełnomocnik ZSZ (audit wewnętrzny) KKO NZP, DLA, DLM, NTE, NIT, DA, DCS, NM, NDG, NKP, NM, NE.
A.15.1.3	Łańcuch dostaw techniki informatycznej i wymiany informacji	Zabezpieczenie Szpitala wyłania dostawców najczęściej poprzez postępowania przetargowe lub wybór ofert. Dokumentacja zawiera wyspecyfikowane wymagani, które musi spełnić dostawca, także w zakresie wymagań technicznych, organizacyjnych i w zakresie komunikacji. Stosowne uregulowania są w dokumentacji przetargowej oraz w umowach z dostawcami.	Audit wewnętrzny, kontrole prowadzone przez organy zwierzchnie	Dyrektor, NG, Pełnomocnik ZSZ (audit wewnętrzny) KKO NZP, DLA, DLM, NTE, NIT, DA, DCS, NM, NDG, NKP, NM, NE.
A.15.2 Zarządzanie dostarczaniem usług			Sposób monitorowania	Odpowiedzialny
Cel: Utrzymanie uzgodnionego poziomu bezpieczeństwa informacji i dostaw usług zgodnie z umowami zawartymi z dostawcami.				
A.15.2.1	Monitorowanie i przegląd usług świadczonych przez dostawców	Zabezpieczenie Usługi w obszarze IT monitorowane i oceniane są przez pracowników NIT. Przed odbiorem usługi w zakresie IT, prowadzone są testy odbiorowe, oraz inne formy weryfikacji w zależności od rodzaju usługi. Kierownik NIT po zakończeniu usługi, ocenia spójność systemów IT.Inne usługi monitorowane i oceniane są przez właściwe Komórki Organizacyjne Szpitala. W szpitalu stosowane są Protokoły obioru.	Audit wewnętrzny	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny). KKO NZP, DLA, DLM, NTE, NIT, DA, DCS, NM, NDG, NKP, NM, NE.
A.15.2.2	Zarządzanie zmianami w usługach świadczonych przez dostawców	Zabezpieczenie Wszelkie zmiany w usługach są zatwierdzane przez Kierowników Komórek Organizacyjnych właściwych komórek organizacyjnych lub Dyrektora Szpitala. Zmiany są wprowadzane w formie aneksów do umów lub dodatkowych zleceń. Na podstawie oceny zmian mogą być wprowadzane aktualizacje w analizie ryzyka oraz w stosowanych zabezpieczeniach.	Audit wewnętrzny, kontrole prowadzone przez organy zwierzchnie W obszarze IT przeglądy prowadzone przez NIT	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny). KKO NZP, DLA, DLM, NTE, NIT, DA, DCS, NM, NDG, NKP, NM, NE.

A.16 Zarządzanie bezpieczeństwem informacji				
A.16.1 Zarządzanie incydentami związanymi z bezpieczeństwem informacji i ulepszeniami			Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie spójnego i efektywnego podejścia do zarządzania incydentami związanymi z bezpieczeństwem informacji, włącznie z wymianą informacji o zdarzeniach związanych z bezpieczeństwem i słabych stronach.				
A.16.1.1	Zakresy obowiązków i procedury	Zabezpieczenie Wymagania określa procedura Postępowania z Incydentami Bezpieczeństwa Informacji.	Audit wewnętrzny	Pełnomocnik ZSZ
A.16.1.2	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	Zabezpieczenie Wymagania określa procedura Postępowania z Incydentami Bezpieczeństwa Informacji. Zdarzenie związane z bezpieczeństwem informacji podlegają zgłoszeniu zgodnie z w/w procedurą.	Audit wewnętrzny	Pełnomocnik ZSZ
A.16.1.3	Zgłaszanie słabych stron bezpieczeństwa informacji	Zabezpieczenie Wymagania określa procedura Postępowania z Incydentami Bezpieczeństwa Informacji. Słabe strony systemu w Szpitalu podlegają zgłoszeniu zgodnie z w/w procedurą.	Audit wewnętrzny	Pełnomocnik ZSZ
A.16.1.4	Szacowanie zdarzeń związanych z bezpie-czeństwem informacji i decyzja	Zabezpieczenie Wymagania określa procedura Postępowania z Incydentami Bezpieczeństwa Informacji. Pracownicy NIT podczas swojej pracy (bieżący monitoring systemu informatycznego, przegląd dziennika logów, prowadzone przeglądy techniczne) oraz wszyscy pracownicy Szpitala mają obowiązek identyfikować wszystkie zdarzenia i słabości i informowania o nich Pełnomocnika. Pełnomocnik ocenia czy zgłoszenie jest incydentem. Jeśli tak to rejestruje je i podejmuje stosowne działania korygujące, podczas który identyfikuje przyczynę.	Audit wewnętrzny,	KKO NIT, ABI, Pełnomocnik ZSZ.
A.16.1.5	Reakcja na incydenty związane z bezpieczeństwem informacji	Zabezpieczenie Wymagania określa procedura Postępowania z Incydentami Bezpieczeństwa Informacji. Działania korygujące nadzoruje Pełnomocnik.Jeśli incydent zagraża ciągłości działania Szpitala, Pełnomocnik może wprowadzić natychmiastowe działania i powiadomić Dyrektora Szpitala, aż do powiadomienia Centrum Zarządzania Kryzysowego.	Audit wewnętrzny	KKO NIT, Pełnomocnik ZSZ. ABI
A.16.1.6	Wyciąganie wniosków z incydentów	Zabezpieczenie Wymagania określa procedura Postępowania z Incydentami Bezpieczeństwa Informacji.	Audit wewnętrzny	Dyrektor, ABI, Pełnomocnik ZSZ, KKO NIT, NM

	związanych z bezpieczeństwem informacji	Podczas prowadzenia działań korygujących, Pełnomocnik ocenia możliwość zdobytych informacji do zredukowania prawdopodobieństwa wystąpienia lub skutków przyszłych incydentów.		
A.16.1.7	Gromadzenie dowodów	Zabezpieczenie W trakcie oceny zdarzeń i słabości związanych z bezpieczeństwem informacji, Pełnomocnik gromadzi i ocenia dowody przekazane przez zgłaszającego. Może też sam wystąpić do poszczególnych Kierownik, o przekazanie dokumentacji i inny dowodów związanych z zgłoszeniem zdarzenia.	Audit wewnętrzny	Dyrektor, ABI, Pełnomocnik ZSZ, KKO NIT, NM
A.17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania				
A.17.1 Ciągłość bezpieczeństwa informacji			Sposób monitorowania	Odpowiedzialny
Cel: Ciągłość bezpieczeństwa informacji powinna być wbudowana w systemy zarządzania ciągłością działania organizacji.				
A.17.1.1	Planowanie ciągłości bezpieczeństwa informacji	Zabezpieczenie Zasady zapewnienia ciągłości działania określone są w Procedurze Zapewnienie ciągłości działania. Zakup infrastruktury informatycznej będzie zrealizowany z rezerw finansowych zarządzania kryzysowego.	Audit wewnętrzny	Dyrektor, ABI, Pełnomocnik ZSZ, KKO NIT, NM
A.17.1.2	Wdrażanie ciągłości bezpieczeństwa informacji	Zabezpieczenie Zasady zapewnienia ciągłości działania określone są w Procedurze Zapewnienie ciągłości działania. Wymagania uregulowano załączniku nr. 1 do Procedury Zapewnienie ciągłości działania - Planie ciągłości działania.	Audit wewnętrzny	Dyrektor, ABI, Pełnomocnik ZSZ, KKO NIT, NM KKO w swoich komórkach organizacyjnych.
A.17.1.3	Weryfikacja, przegląd i ocena ciągłości bezpieczeństwa informacji	Zabezpieczenie Zasady zapewnienia ciągłości działania określone są w Procedurze Zapewnienie ciągłości działania, w tym zasady weryfikacji (testów) . Aktualność procedury oceniana jest podczas oceny zgodności dokumentacji ZSZ.	Audit wewnętrzny	Pełnomocnik ZSZ, KKO NIT, NM. KKO w swoich komórkach organizacyjnych.
A.17.2 Rezerwowanie			Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie dostępności środków przetwarzania informacji.				

A.17.2.1	Dostępność środków przetwarzania informacji	Zabezpieczenie Rezerwowymi środkami przetwarzania (takimi jak stacje robocze) dysponuje dział NIT, w wyjątkowych przypadkach w porozumieniu z Kierownik, mogą zostać przesunięte środki przetwarzania między poszczególnymi KO Szpitala. W sytuacjach kryzysowych ma zastosowanie Procedura Zapewnienie ciągłości działania. NIT ma obowiązek zapewnienia odpowiednich zasobów informatycznych do realizacji zadań Szpitala w ramach przydzielonych środków finansowych.	Audit wewnętrzny Przeglądu infrastruktury informatycznej.	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny)
A.18 Zgodność				
A.18.1 Zgodność z wymaganiami prawnymi i umownymi			Sposób monitorowania	Odpowiedzialny
Cel: Uniknięcie naruszeń zobowiązań prawnych, ustawowych, regulaminowych lub umownych związanych z bezpieczeństwem informacji oraz wszelkich wymagań dotyczących bezpieczeństwa.				
A.18.1.1	Identyfikacja obowiązującego ustawodawstwa i wymagań umownych	Zabezpieczenie Za ocenę zgodności prawnej odpowiedzialni są Kierownicy Komórek Organizacyjnych komórek organizacyjnych, każdy w swoim zakresie.	Audit wewnętrzny	KKO w swoich komórkach organizacyjnych. Pełnomocnik ZSZ (audit wewnętrzny)
A.18.1.2	Prawa własności intelektualnej	Zabezpieczenie W szpitalu stosuje się oprogramowanie zgodnie z udzielonymi na nie licencjami. Dowody legalności oprogramowania przechowuje NIT.	Audit wewnętrzny	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny)
A.18.1.3	Ochrona zapisów	Zabezpieczenie Dostęp do zapisów mają pracownicy zgodnie z zakresem odpowiedzialności i upoważnieniami do przetwarzania danych osobowych oraz nadanym dostępem do zasobów serwerów. Zapisy papierowe przechowywane są w oznaczonych segregatorach lub szafach. Zasady określono w Standardzie NIT (zapisy elektroniczne) oraz w ramach nadzoru na informacją udokumentowaną..	Audit wewnętrzny Przeglądu infrastruktury informatycznej.	KKO NIT. KKO w swoich komórkach organizacyjnych. Pełnomocnik ZSZ (audit wewnętrzny)
A.18.1.4	Prywatność i ochrona informacji umożliwiających ujawnienie tożsamości	Zabezpieczenie W organizacji wdrożono zasady Ochrony Danych Osobowych w tym Dokumentację Ochrony Danych Osobowych zgodnie z obowiązującymi wymaganiami prawnymi	Audit wewnętrzny Inspekcje (co najmniej raz na 5 lat)	ABI, KKO w swoich komórkach organizacyjnych. Pełnomocnik ZSZ (audit wewnętrzny)

A.18.1.5	Regulacje dotyczące zabezpieczeń kryptograficznych	Zabezpieczenie Zasady określono w zabezpieczeniach serii A 10. Szpital stosuje zabezpieczenia kryptograficzne w komunikacji z Organizacjami zewnętrznymi zgodnie z wymaganiami prawnymi oraz umownymi (Banki)	Audit wewnętrzny	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny)
A.18.2 Przeglądy bezpieczeństwa informacji			Sposób monitorowania	Odpowiedzialny
Cel: Zapewnienie że bezpieczeństwo informacji jest wdrożone i działa zgodnie z politykami i procedurami organizacyjnymi.				
A.18.2.1	Niezależny przegląd bezpieczeństwa informacji	Zabezpieczenie W Szpitalu prowadzone są zaplanowane audity wewnętrzne w celu oceny zgodności przetwarzania informacji. W auditach według potrzeb mogą być powoływani audytorzy z zewnątrz. Raz w roku w ramach certyfikacji, niezależny audit SZBI prowadzi jednostka certyfikacyjna.	Audit wewnętrzny	Dyrektor, Pełnomocnik ZSZ
A.18.2.2	Zgodność z politykami bezpieczeństwa i normami	Zabezpieczenie Kierownicy Komórek Organizacyjnych, każdy w swoim zakresie oraz Pełnomocnik są odpowiedzialni za przestrzeganie i monitorowanie stosowania zasad określonych w dokumentacji SZBI oraz wymagań zawartych w normach, zarządzania oraz przepisach prawnych. Kierownicy Komórek Organizacyjnych oceniają zgodność w tym zakresie, nadzorując pracę komórek organizacyjnych. O wszelkich nieprawidłowościach informują. Pełnomocnik ocenia zgodność przetwarzania informacji na auditach wewnętrznych.	Audit wewnętrzny	KKO w swoich komórkach organizacyjnych. Pełnomocnik ZSZ (audit wewnętrzny)
A.18.2.3	Przegląd zgodności technicznej	Zabezpieczenie Pod względem organizacyjnym nadzór nad zgodnością przetwarzania prowadzi na bieżąco Kierownik NIT. Przeglądy techniczne krytycznej infrastruktury IT prowadzi Dział NIT co najmniej raz w roku.	Audit wewnętrzny Przegląd infrastruktury informatycznej.	KKO NIT, Pełnomocnik ZSZ (audit wewnętrzny)