POWIATOWE CENTRUM ZDROWIA Sp. z o. o.
W LWÓWKU ŚLĄSKIM
UL. MORCINKA 7, TEL. 075 782 01 04

DEKLARACJA STOSOWANIA

Numer referencyjny procedury:	9/2022/PI
Data wprowadzenia**:**	30.09.2022
Data ewaluacji:	
Miejsce zastosowania:	Powiatowe Centrum Zdrowia Sp. z o. o. z siedzibą w Lwówku Śląskim
Opracowane przez:	Monika Śmieszek Inspektor Ochrony Danych Osobowych
Sprawdzone przez:	Maciej Lech Pełnomocnik ds. Zintegrowanego Systemu Zarządzania
Zatwierdzono przez:	

Załącznik A (Deklaracja stosowania)

Sporządził :	Sprawdził:	Zatwierdził:

WZORCOWY WYKAZ CELÓW STOSOWANIA ZABEZPIECZEŃ i ZABEZPIECZENIA

Tabela A.1 – Cele stosowania zabezpieczeń i zabezpieczenia

A.5 Polityki bezpieczeństwa informacji		
A.5.1 Kierunki bezpieczeństwa informacji określane przez kierownictwo		
Cel: Zapewnienie przez kierownictwo wytycznych i wsparcia dla działań na rzecz bezpieczeństwa informacji, zgodnie z wymaganiami biznesowymi oraz właściwymi normami prawnymi i regulacjami.		
A.5.1.1	Polityki bezpieczeństwa informacji	*Zabezpieczenie* Powiatowe Centrum Zdrowia Sp. z o. o. posiada zatwierdzoną przez Zarząd Politykę Bezpieczeństwa Informacji, która została opublikowana i jest dostępna, w odpowiednim zakresie, dla wszystkich pracowników i stron zewnętrznych znajdujących się w siedzibie Spółki. Polityka zawiera cele ochrony oraz zobowiązanie Zarządu Spółki do zapewnienia środków do realizacji polityki, potwierdza również, że zarządzanie bezpieczeństwem odbywa się zgodnie z przepisami prawa oraz regulacjami wewnętrznymi.
A.5.1.2	Przegląd polityk bezpieczeństwa informacji	*Zabezpieczenie* Polityka Bezpieczeństwa Informacji w Spółce jest poddawana regularnym przeglądom pod kątem jej przydatności, adekwatności i efektywności w trakcie przeprowadzania przeglądów zarządzania.
A.6 Organizacja bezpieczeństwa informacji		
A.6.1 Organizacja wewnętrzna		
Cel: Ustanowić strukturę zarządzania w celu zainicjowania oraz nadzorowania wdrażania i eksploatacji bezpieczeństwa informacji w organizacji.		
A.6.1.1	Role i odpowiedzialność za bezpieczeństwo informacji	*Zabezpieczenie* Role w bezpieczeństwie informacji i zakresy odpowiedzialności pracowników zostały określone i zapisane w zakresach czynności pracowników dla poszczególnych stanowisk. Koordynacja bezpieczeństwa informacji w Spółce jest zapewniona dzięki powołaniu Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych.

A.6.1.2	Rozdzielenie obowiązków	*Zabezpieczenie* Wszyscy pracownicy Spółki mają przypisaną odpowiedzialność za bezpieczeństwo informacji, która została określona w oświadczeniach o zachowaniu poufności. Dodatkowo, odpowiedzialności te określone zostały w dokumentacji funkcjonującej w ramach Systemu Zrządzania Bezpieczeństwem Informacji.
A.6.1.3	Kontakty z organami władzy	*Zabezpieczenie* Spółka utrzymuje stosowne kontakty z organami władzy w zakresie wymaganym prawem.
A.6.1.4	Kontakty z grupami zainteresowanych specjalistów	*Zabezpieczenie* Wybrani pracownicy utrzymują na bieżąco kontakty z grupami zaangażowanymi w zapewnienie bezpieczeństwa poprzez śledzenie grup dyskusyjnych oraz portali poświęconych bezpieczeństwu informacji.
A.6.1.5	Bezpieczeństwo informacji w zarządzaniu projektami.	*Zabezpieczenie* Każdy projekt realizowany w Spółce jest oceniany przez Inspektora Ochrony Danych pod kątem 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	*Zabezpieczenie* Formalne zasady postępowania z urządzeniami mobilnymi zdefiniowane zostały w dokumencie „Ogólne zasady bezpieczeństwa informacji”.
A.6.2.2	Telepraca	*Zabezpieczenie* W Spółce w odniesieniu do usług związanych z telepracą jest stroną będącą klientem, w związku z czym stsuje standardowe zabezpieczenia oferowane przez zarządzających tymi usługami.

A.7 Bezpieczeństwo zasobów ludzkich		
A.7.1 Przed zatrudnieniem		
Cel: Zapewnić, żeby pracownicy i kontrahenci zrozumieli swoją odpowiedzialność i byli odpowiednimi kandydatami do wypełnienia ról, do których są przewidziani.		
A.7.1.1	Postępowanie sprawdzające	*Zabezpieczenie* Zasady postępowania przy rekrutacji nowych pracowników zostały zdefiniowane w „Procedurze zarządzania zasobami ludzkimi”.
A.7.1.2	Warunki zatrudnienia	*Zabezpieczenie* Pracownicy mają zdefiniowane odpowiedzialności za zachowanie bezpieczeństwa informacji w podpisywanych przez nich oświadczeniach o zachowaniu 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	*Zabezpieczenie* Kierownictwo jest odpowiedzialne za nadzór nad podległymi pracownikami i kontrahentami w zakresie realizacji wymagań wynikających z wdrożonego Zintegrowanego Systemu Zarządzania Jakością.
A.7.2.2	Uświadomienie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	*Zabezpieczenie* Pracownicy Spółki przechodzą szkolenia z zakresu bezpieczeństwa informacji oraz na bieżąco i regularnie informowani są o zmianach wymagań zawartych w dokumentacji Systemu Zrządzania Bezpieczeństwem Informacji. W tym celu wykorzystuje się spotkania wewnętrzne (odprawy), system systematycznych, krótkich szkoleń.
A.7.2.3	Postępowanie dyscyplinarne	*Zabezpieczenie* Zasady postępowania dyscyplinarnego określone zostały w „Procedurze zarządzania zasobami ludzkimi” oraz instrukcji „Ogóle zasady bezpieczeństwa informacji”.

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 zmianą zatrudnienia	*Zabezpieczenie* Odpowiedzialności związane z zakończeniem lub zmianą zatrudnienia zdefiniowane zostały w „Procedurze zarządzania zasobami ludzkimi”.
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	*Zabezpieczenie* Aktywa informacyjne zostały zinwentaryzowane i zestawione w dokumencie „Wykaz aktywów”.
A.8.1.2	Własność aktywów	*Zabezpieczenie* Własność aktywów fizycznych i programowych została przypisana do osób nimi dysponujących, własność aktywów informacyjnych została zdefiniowana w dokumencie „Wykaz aktywów”.
A.8.1.3	Akceptowalne użycie aktywów	*Zabezpieczenie* Zasady dotyczące akceptowalnego użycia aktywów opisane zostały w Instrukcji „Ogólne zasady bezpieczeństwa informacji” oraz w Polityce Bezpieczeństwa dla Systemów Informatycznych Służących do Przetwarzania Danych Osobowych.
A.8.1.4	Zwrot aktywów	*Zabezpieczenie* Wszyscy pracownicy oraz podmioty zewnętrzne zwracają wszystkie aktywa należące do Spółki, a będące w ich posiadaniu, w momencie ustania zatrudnienia, umowy lub porozumienia.
A.8.2 Klasyfikacja informacji		
Cel: Zapewnić przypisanie informacjom odpowiedniego poziomu ochrony, zgodnego z ich wagą dla organizacji.		
A.8.2.1	Klasyfikowanie informacji	*Zabezpieczenie* W Spółce funkcjonuje procedura „Klasyfikacja informacji” przedstawiająca sposób sklasyfikowania informacji uwzględniający ich wartości dla organizacji.

A.8.2.2	Oznaczanie informacji	*Zabezpieczenie* Procedura „Klasyfikacja informacji" określa zasady dotyczące oznaczania i postępowania z informacjami funkcjonującymi w Szpitalu .
A.8.2.3	Postępowanie z aktywami	*Zabezpieczenie* Zasady postępowania z aktywami określone zostały w instrukcji „Ogóle zasady bezpieczeństwa informacji".
A.8.3 Postępowanie z nośnikami		
Cel: Zapobiec nieuprawnionemu ujawnianiu, modyfikacji, usunięciu lub zniszczeniu informacji zapisanych na nośnikach.		
A.8.3.1	Zarządzanie nośnikami wymiennymi	*Zabezpieczenie* Formalne zasady postępowania z nośnikami wymiennymi zdefiniowane zostały w dokumencie „Ogólne zasady bezpieczeństwa informacji".
A.8.3.2	Wycofywanie nośników	*Zabezpieczenie* Zasady niszczenia nośników zostały zdefiniowane w dokumencie „Ogólne zasady bezpieczeństwa informacji".
A.8.3.3	Przekazywanie nośników	*Zabezpieczenie* Zasady transportowania nośników określone zostały w odpowiednich umowach.
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	*Zabezpieczenie* W Spółce zdefiniowano i przydzielono zakresy dostępu do usług i aplikacji zgodnie z zasadami określonymi w „Procedurze zarządzania uprawnieniami".
A.9.2 Zarządzanie dostępem użytkowników		
Cel: Zapewnić dostęp uprawnionym użytkownikom i zapobiec nieuprawnionemu dostępowi do systemów i usług		
A.9.2.1	Rejestracja i wyrejestrowanie użytkowników	*Zabezpieczenie* Zasady związane z rejestracją i wyrejestrowaniem użytkowników przetwarzających dane określone zostały w „Procedurze zarządzania uprawnieniami".

A.9.2.2	Przydzielanie dostępu użytkowników	*Zabezpieczenie* Zasady związane z zapewnieniem dostępu użytkowników do informacji określone zostały w „Procedurze zarządzania uprawnieniami”.
A.9.2.3	Zarządzanie prawami uprzywilejowanego dostępu	*Zabezpieczenie* Zasady związane z rejestracją użytkowników przetwarzających dane określone zostały w „Procedurze zarządzania uprawnieniami”.
A.9.2.4	Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników	*Zabezpieczenie* Zasady związane z zarządzaniem poufnymi informacjami uwierzytelniającymi użytkowników określa „Polityka Bezpieczeństwa“.
A.9.2.5	Przegląd praw dostępu użytkowników	*Zabezpieczenie* Zasady związane z przeglądem praw dostępu użytkowników określone zostały w „Procedurze zarządzania uprawnieniami”.
A.9.2.6	Odbieranie lub dostosowywanie praw dostępu	*Zabezpieczenie* Zasady związane z odebraniem lub dostosowaniem praw dostępu użytkowników określone zostały w „Procedurze zarządzania uprawnieniami”.
A.9.3 Odpowiedzialność użytkowników		
Cel: Zapewnić rozliczalność użytkowników w celu ochrony ich informacji uwierzytelniających.		
A.9.3.1	Stosowanie poufnych informacji uwierzytelniających	*Zabezpieczenie* Zasady związane z zarządzaniem poufnymi informacjami uwierzytelniającymi użytkowników określa „Polityka Bezpieczeństwa“.
A.9.4 Kontrola dostępu do systemu i aplikacji		
Cel: Zapobiec nieuprawnionemu dostępowi do systemów i aplikacji.		
A.9.4.1	Ograniczenie dostępu do informacji	*Zabezpieczenie* Zabezpieczenie to jest stosowane w przypadku systemów informatycznych – poszczególni użytkownicy mają dostęp do informacji na poziomie zdefiniowanym przez administratora systemów.
A.9.4.2	Procedury bezpiecznego logowania	*Zabezpieczenie* Systemy operacyjne na stacjach roboczych wykorzystywanych w Spółce wymagają identyfikacji i uwierzytelnienia użytkownika.

A.9.4.3	System zarządzania hasłami	*Zabezpieczenie* Dla wybranych systemów informatycznych zarządzanie hasłami odbywa się przy wykorzystaniu polityki haseł zgodnie z dokumentem „Polityka bezpieczeństwa”
A.9.4.4	Użycie uprzywilejowanych programów narzędziowych	*Zabezpieczenie* Sysytemowe programy narzędziowe stosowane są tylko przez uprawnione osoby z zespołu informatyków.
A.9.4.5	Kontrola dostępu do kodów źródłowych programów	*Zabezpieczenie* Nie ma zastosowania. Spółka korzysta z programów autorstwa podmiotów zewnętrznych.
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	*Zabezpieczenie* Zabezpieczenia kryptograficzne są stosowane w odniesieniu do wybranych serwerów. W szczególnych przypadkach w Spółce stosowane są podpisy elektroniczne.
A.10.1.2	Zarządzanie kluczami	*Zabezpieczenie* Zasady związane z zarządzaniem kluczami określa „Procedura Zarządzanie Uprawnieniami“ i instrukcja „Zarządzanie kluczami do pomieszczeń“
A.11 Bezpieczeństwo fizyczne i środowiskowe		
A.11.1 Obszary bezpieczne		
Cel: Zapobiec nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w informacji i środkach przetwarzania informacji należących do organizacji.		
A.11.1.1	Fizyczna granica obszaru bezpiecznego	*Zabezpieczenie* Szpital zlokalizowany jest w trzech budynkach. Dostęp z zewnątrz możliwy jest poprzez główne wejście oraz szereg wejść dodatkowych. Pełniony jest również nadzór wizyjny nad wybranym fragmentem budynków przy użyciu kamer.

A.11.1.2	Fizyczne zabezpieczenie wejść	*Zabezpieczenie* Po godzinach pracy dostęp do pomieszczeń Szpitala odbywa się przez wejście do Izby przyjęć. Okresową inspekcję terenu Szpitala wykonują pracownicy Działu Technicznego. W przypadku zagrożeń wzywana jest firma ochroniarska, policja.
A.11.1.3	Zabezpieczenie biur, pomieszczeń i obiektów	*Zabezpieczenie* Budynek Szpitala jest podzielony na formalne strefy bezpieczeństwa. Dostęp do nich jest przydzielany w sformalizowany sposób. Pomieszczenia nie objęte zamkami szyfrowymi zamykane są przy pomocy kluczy mechanicznych. Dostęp do pomieszczeń strefy I jest ograniczony. Stosuje się dodatkowe zabezpieczenia.
A.11.1.4	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	*Zabezpieczenie* Organizacja stosuje system wykrywania pożaru oparty na detektorach dymu okresowo testowanych. Gaśnice i hydranty są weryfikowane pod kątem ich sprawność.
A.11.1.5	Praca w obszarach bezpiecznych	*Zabezpieczenie* Zasady pracy w obszarach chronionych zostały sformalizowane w procedurze „Ogóle zasady bezpieczeństwa informacji”
A.11.1.6	Obszary dostaw i załadunku	*Zabezpieczenie* Obszarem publicznie dostępnym są pomieszczenia holi i korytarzy.
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	*Zabezpieczenie* Sprzęt przetwarzający informacje rozlokowany jest w sposób ograniczający dostęp osób postronnych.
A.11.2.2	Systemy wspomagające	*Zabezpieczenie* Szpital korzysta z systemów UPS obejmujących: • Sale operacyjne • OIOM • Serwerownie Źródło zasilania w przypadku wystąpienia awarii przełączane jest automatycznie na UPS, który jest okresowo testowany i dozorowany. W przypadku zaniku zasilania automatycznie uruchamiany jest zespół agregatów prądotwórczych. W serwerowni zainstalowano klimatyzatory, z których praca wystarcza do zapewnienia właściwych warunków eksploatacji. Temperatura i wilgotność powietrza jest monitorowana na bieżąco.

A.11.2.3	Bezpieczeństwo okablowania	*Zabezpieczenie* Okablowanie sieci komputerowej w Szpitalu jest rozłożone w torach kablowych (plastikowych korytkach) minimalizujących ryzyko ich przypadkowego uszkodzenia.
A.11.2.4	Konserwacja sprzętu	*Zabezpieczenie* Urządzenia konserwowane są przez pracowników zespołu informatyków zgodnie z wewnętrznymi potrzebami lub za pośrednictwem podmiotów zewnętrznych na podstawie stosownych umów.
A.11.2.5	Wynoszenie aktywów	*Zabezpieczenie* Zasady dotyczące postępowania ze sprzętem przenośnym oraz dokumentami określa „Ogólne zasady bezpieczeństwa informacji”.
A.11.2.6	Bezpieczeństwo sprzętu i aktywów poza siedzibą	*Zabezpieczenie* W organizacji używane są komputery przenośne. Zasady dotyczące postępowania ze sprzętem przenośnym określa procedura „Ogólne zasady bezpieczeństwa informacji”.
A.11.2.7	Bezpieczne zbywanie lub przekazywanie do ponownego użycia	*Zabezpieczenie* Zasady wykorzystania i niszczenia nośników informacji określono w instrukcji „Ogólne zasady bezpieczeństwa informacji”.
A.11.2.8	Pozostawienie sprzętu użytkownika bez opieki	*Zabezpieczenie* Wymagania w zakresie pozostawiania sprzętu użytkownika bez opieki zostały zdefiniowane w instrukcji „Ogólne zasady bezpieczeństwa informacji”.
A.11.2.9	Polityka czystego biurka i czystego ekranu	*Zabezpieczenie* Zasady dotyczące przechowywania dokumentów i nośników wymiennych zostały zdefiniowane w dokumencie „Ogólne zasady bezpieczeństwa informacji”. Polityka czystego ekranu realizowana jest na wszystkich stacjach roboczych, na których skonfigurowano wygaszacz w taki sposób, by jego wyłączenie było możliwe poprzez podanie hasła.
A.12 Bezpieczna eksploatacja		
A.12.1 Procedury eksploatacyjne i odpowiedzialność		
Cel: Zapewnić poprawną i bezpieczną eksploatacją środków przetwarzania informacji.		
A.12.1.1	Dokumentowanie procedur eksploatacyjnych	*Zabezpieczenie* Zasady dotyczące eksploatacji systemów zostały udokumentowane.

A.12.1.2	Zarządzanie zmianami	*Zabezpieczenie* Wprowadzanie wszelkich zmian w systemach realizowane jest zgodnie z „Procedurą zarządzania zmianami w systemach informatycznych”.
A.12.1.3	Zarządzanie pojemnością	*Zabezpieczenie* Organizacja monitoruje wydajność wybranych systemów informatycznych m.in. w zakresie pojemności dysków Sewerów oraz mocy obliczeniowej procesorów serwerów.
A.12.1.4	Rozdzielenie środowisk rozwojowych, testowych i produkcyjnych	*Zabezpieczenie* Dla wybranych środowisk zdefiniowano urządzenia/ środowiska testowe i rozwojowe. Opierając się na inwentaryzacji systemów informatycznych i szacowaniu ryzyka wytypowano systemy dla których niezbędne jest istnienie środowisk rozwojowych i testowych.
A.12.2 Ochrona przed szkodliwym oprogramowaniem		
Cel: Zapewnić informacjom i środkom przetwarzania informacji ochroną przed szkodliwym oprogramowaniem.		
A.12.2.1	Zabezpieczenia przed szkodliwym oprogramowaniem	*Zabezpieczenie* W Szpitalu stosuje się oprogramowanie antywirusowe Comodo. Ochroną objęte są zarówno serwery jak i stacje robocze. Oprogramowanie skonfigurowano do automatycznej aktualizacji baz sygnatur. Zabezpieczenie przed informacją pochodzącą z nieautoryzowanych źródeł np. Internet istnieje dwustopniowy system ochrony (filtr na firewallu i program antywirusowy).
A.12.3 Kopie zapasowe		
Cel: Chronić przed utratą danych.		
A.12.3.1	Zapasowe kopie informacji	*Zabezpieczenie* W Szpitalu wykonuje się kopie zapasowe. Zasady odnośnie tworzenia, przechowywania i przenoszenia kopii zostały sformalizowane w procedurze „Ogólne zasady bezpieczeństwa informacji”. Do tworzenia kopii zapasowych wykorzystuje płyty DVD/BD dyski HD, pamięci taśmowe oraz serwery plików.

A.12.4 Rejestrowanie zdarzeń i monitorowanie		
Cel: Rejestrować zdarzenia i zbierać materiał dowodowy.		
A.12.4.1	Rejestrowanie zdarzeń	*Zabezpieczenie* Rejestrowanie zdarzeń odbywa się automatycznie i w przypadku błędów krytycznych jest przesyłanie do dostawców oprogramowania
A.12.4.2	Ochrona informacji zawartych w dziennikach zdarzeń	*Zabezpieczenie* Dzienniki audytu objęte są standardowymi mechanizmami ochrony na każdym z serwerów wykorzystywanych w sieci Szpitala.
A.12.4.3	Rejestrowanie działań administratorów i operatorów	*Zabezpieczenie* Dla wybranych systemów stosuje się dzienniki np. dla serwerów bazodanowych..
A.12.4.4	Synchronizacja zegarów	*Zabezpieczenie* Komputery posiadają wewnętrzne zegary czasu, które są synchronizowane z zewnętrznym źródłem czasu.
A.12.5 Nadzór nad oprogramowaniem produkcyjnym		
Cel: Zapewnić integralność systemów produkcyjnych		
A.12.5.1	Instalacja oprogramowania w systemach produkcyjnych	*Zabezpieczenie* Instalacje oprogramowania dokonywane jest przez upoważniony, posiadający właściwe kompetencje personel.
A.12.6 Zarządzanie podatnościami technicznymi		
Cel: Zapobiec wykorzystywaniu podatności technicznych.		
A.12.6.1	Zarządzanie podatnościami technicznymi	*Zabezpieczenie* 1. Administratorzy serwerów na bieżąco zapoznają się z informacjami dotyczącymi zidentyfikowanych nowych podatności technicznych wykorzystywanego oprogramowania i podejmują stosowne działania. 2. W Szpitalu zarządza się w sposób systemowy poprawkami systemów operacyjnych stacji roboczych.
A.12.6.2	Ograniczenia w instalowaniu oprogramowania	*Zabezpieczenie* Instalacje oprogramowania dokonywane jest przez upoważniony, posiadający właściwe kompetencje personel.

A.12.7 Rozważania dotyczące audytu systemów informacyjnych		
Cel: Zminimalizować wpływ działań audytu na systemy produkcyjne		
A.12.7.1	Zabezpieczenia audytu systemów informacyjnych	*Zabezpieczenie* Systemy Szpitala podlegają przeglądom realizowanym zgodnie z zapisami w zintegrowanej księdze zarządzania.
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	Zabezpieczenie sieci	*Zabezpieczenie* Sieci są zarządzane i nadzorowane aby chronić informacje w systemach i aplikacjach.
A.13.1.2	Bezpieczeństwo usług sieciowych	*Zabezpieczenie* Zasady związane z przeglądem praw dostępu użytkowników określone zostały w „Procedurze zarządzania uprawnieniami”.
A.13.1.3	Rozdzielanie sieci	*Zabezpieczenie* W Szpitalu nie stosuje się rozdzielania sieci wewnętrznej na podsieci.
A.13.2 Przekazywanie informacji		
Cel: Utrzymać bezpieczeństwo informacji przesyłanych wewnątrz organizacji i wymienianych z podmiotami zewnętrznymi.		
A.13.2.1	Polityki i procedury przesyłania informacji	*Zabezpieczenie* Procedury i zasady bezpiecznej wymiany informacji w Szpitalu są opisane w dokumentacji Systemu Zrządzania Bezpieczeństwem Informacji.
A.13.2.2	Porozumienia dotyczące przesyłaniu informacji	*Zabezpieczenie* Szpitalu stosuje standardy wymiany informacji z głównymi dostawcami usług. Standardy te zostały zdefiniowane w umowach o świadczenie usług.
A.13.2.3	Wiadomości elektroniczne	*Zabezpieczenie* W Szpitalu wdrożono systemy antywirusowe na stacjach roboczych oraz na serwerze poczty (serwer zewnętrzny nawa.pl), dzięki czemu wiadomości, w tym także załączniki, sprawdzane są pod kątem zawartości oprogramowania szkodliwego.

A. 13.2.4	Umowy o zachowaniu poufności	*Zabezpieczenie* Dostęp do stosownych systemów nadawany jest tylko uprawnionym osobom.
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	*Zabezpieczenie* Szpital analizuje, definiuje i wdraża konieczne do zaimplementowania w systemach mechanizmy bezpieczeństwa.
A.14.1.2	Zabezpieczanie usług aplikacyjnych w sieciach publicznych	*Zabezpieczenie* Wymagania związane z bezpieczeństwem informacji zawarte są w wymaganiach dla nowych systemów informacyjnych lub rozszerzeń dla istniejących systemów informacyjnych.
A.14.1.3	Ochrona transakcji usług aplikacyjnych	*Zabezpieczenie* Szpital korzystając z aplikacji usługowych jest klientem, w związku z czym stosuje standardowe zabezpieczenia oferowane przez zarządzających tymi usługami.
A.14.2 Bezpieczeństwo w procesach rozwojowych i wsparcia		
Cel: Zapewnić projektowanie i wdrożenie bezpieczeństwa informacji w ramach cyklu życia systemów informacyjnych.		
A.14.2.1	Polityka bezpieczeństwa prac rozwojowych	*Zabezpieczenie* W Szpitalu zostały ustanowione i są stosowane zasady dotyczące rozwoju oprogramowania.
A.14.2.2	Procedury kontroli zmian w systemach	*Zabezpieczenie* Zasady dokonywania zmian w systemie określone zostały w „Procedurze zarządzania zmianami w systemach informatycznych”
A.14.2.3	Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	*Zabezpieczenie* Zmiany w systemie operacyjnym lub zmiany w środowisku poprzedzone są odpowiednimi testami.

A.14.2.4	Ograniczenia dotyczące zmian w pakietach oprogramowania	*Zabezpieczenie* Zasady dokonywania zmian w pakietach oprogramowania określone zostały w „Procedurze zarządzania zmianami w systemach informatycznych”
A.14.2.5	Zasady projektowania bezpiecznych systemów	*Zabezpieczenie* Zastosowano system ochrony antywirusowej, nadzór nad uprawnieniami użytkowników (realizowany przez ich przełożonych),
A.14.2.6	Bezpieczne środowisko rozwojowe	*Zabezpieczenie* Szpital dąży do zapewnienia bezpiecznego środowiska do rozwoju i integracji systemu w całym cyklu rozwojowym.
A.14.2.7	Prace rozwojowe powierzone podmiotom zewnętrznym	*Zabezpieczenie* Szpital korzysta wyłącznie z usług renomowanych dostawców oprogramowania.
A.14.2.8	Testowanie bezpieczeństwa systemów	*Zabezpieczenie* Na poszczególnych etapach prac rozwojowych prowadzone są testy funkcjonalności bezpieczeństwa systemu.
A. 14.2.9	Testy akceptacyjne systemów	*Zabezpieczenie* Po zakończeniu prac związanych z wdrażaniem nowych lub modernizacją już istniejących systemów informacyjnych przeprowadzane są testy odbiorcze.
A.14.3 Dane testowe		
Cel: Zapewnić ochronę danych stosowanych do testów		
A.14.3.1	Ochrona danych testowych	*Zabezpieczenie* Zakres testów jest starannie dobrany, a ich wyniki są chronione.
A.15 Relacje z dostawcami		
A.15.1 Bezpieczeństwo informacji w relacjach z dostawcami		
Cel: Zapewnić ochronę aktywów organizacji udostępnianych dostawcom.		
A.15.1.1	Polityka bezpieczeństwa informacji w relacjach z dostawcami	*Zabezpieczenie* W umowach z dostawcami zawarte są wymagania dotyczące bezpieczeństwa informacji ograniczające ryzyko związane z ich dostępem do aktywów Szpitala.

A.15.1.2	Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami.	*Zabezpieczenie* Wszystkie istotne wymagania dotyczące bezpieczeństwa informacji uzgodnione z każdym dostawcą, który może mieć do nich dostęp, może je przetwarzać zawarte są w umowach.
A.15.1.3	Łańcuch dostaw technologii informacyjnych i komunikacyjnych	*Zabezpieczenie* Umowy z dostawcami zawierają wymagania określające ryzyko utraty informacji związane z dostawą wyrobów wykorzystywanych przy świadczeniu usług informacyjnych i komunikacyjnych.
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.	*Zabezpieczenie* Komórki organizacyjne odpowiedzialne za usługi informatyczne dostarczane przez strony trzecie mają obowiązek nadzoru nad ich poziomem.
A.15.2.2	Zarządzanie zmianami w usługach świadczonych przez dostawców	*Zabezpieczenie* Szpital korzysta z gotowych produktów. Obowiązuje co najmniej umowa o nadzorze autorskim lub serwisie.
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 zarzadzania incydentami związanymi z bezpieczeństwem informacji z uwzględnieniem informowania o zdarzeniach i słabościach.		
A.16.1.1	Odpowiedzialność i procedury	*Zabezpieczenie* Odpowiedzialności za obsługę incydentów bezpieczeństwa definiuje „Procedura zarządzania incydentami bezpieczeństwa informacji“
A.16.1.2	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	*Zabezpieczenie* W Szpitalu funkcjonuje „Procedura zarządzania incydentami bezpieczeństwa informacji“ definiująca zasady zgłaszania zdarzeń związanych z bezpieczeństwem informacji.
A.16.1.3	Zgłaszanie słabości związanych z bezpieczeństwem informacji	*Zabezpieczenie* W Szpitalu funkcjonuje procedura „Procedura zarządzania incydentami bezpieczeństwa informacji“ definiująca zasady zgłaszania słabości systemu bezpieczeństwa.

A.16.1.4	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji	*Zabezpieczenie* W Szpitalu funkcjonuje procedura „Procedura zarządzania incydentami bezpieczeństwa informacji“ określająca sposób oceniania i podejmowania decyzji w przypadku wystąpienia incydentu bezpieczeństwa informacji.
A.16.1.5	Reagowanie na incydenty związane z bezpieczeństwem informacji	*Zabezpieczenie* W Szpitalu funkcjonuje procedura „Procedura zarządzania incydentami bezpieczeństwa informacji“ określająca sposób reagowania w przypadku wystąpienia incydentu bezpieczeństwa informacji.
A.16.1.6	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji	*Zabezpieczenie* Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji jest zapewnione dzięki realizacji wymagań „Procedury zarządzania incydentami bezpieczeństwa informacji“
A.16.1.7	Gromadzenie materiału dowodowego	*Zabezpieczenie* Zasady gromadzenia materiału dowodowego określone zostały w „Procedura zarządzania incydentami bezpieczeństwa informacji“
A.17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania		
A.17.1 Ciągłość bezpieczeństwa informacji		
Cel: Zaleca się uwzględnienie ciągłości bezpieczeństwa informacji w systemach zarzadzania ciągłością działania organizacji.		
A.17.1.1	Planowanie ciągłości bezpieczeństwa informacji	*Zabezpieczenie* Wymagania bezpieczeństwa są elementem planu ciągłości działania.
A.17.1.2	Wdrażanie ciągłości bezpieczeństwa informacji	*Zabezpieczenie* Opracowano „Procedurę zarządzania ciągłością działania” oraz szablon planu ciągłości działania uwzględniający bezpieczeństwo informacji.
A.17.1.3	Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji	*Zabezpieczenie* Zasady testowania, utrzymania i oceny planów ciągłości działania określone zostały w „Procedurze zarządzania ciągłością działania”.

A.17.2 Nadmiarowość		
Cel: Zapewnić dostępność środków przetwarzania informacji.		
A.17.1.2	Dostępność środków przetwarzania informacji	*Zabezpieczenie* Środki przetwarzania informacji są przystosowane i uwzględniają redundancję wystarczającą do spełnienia wymagań dostępności.
A.18 Zgodność		
A.18.1 Zgodność z przepisami prawnymi i umowami		
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	*Zabezpieczenie* Odpowiedzialność za identyfikację przepisów prawnych spoczywa na Radcy Prawnym. Radcy Prawni wspomagają wszystkie komórki w zidentyfikowaniu odpowiednich przepisów prawnych oraz wymagań wynikających z umów a dotyczących pracy Szpitala .
A.18.1.2	Prawa własności intelektualnej	*Zabezpieczenie* Administratorzy systemów odpowiadają za nadzorowanie ilości i aktualności posiadanych licencji na oprogramowanie.
A.18.1.3	Ochrona zapisów	*Zabezpieczenie* W Szpitalu zapisy organizacji chronione są zgodnie z wymaganiami prawnymi oraz wymaganiami Systemu Zrządzania Bezpieczeństwem Informacji.
A.18.1.4	Prywatność i ochrona danych identyfikujących osobę	*Zabezpieczenie* Wymagania związane z przetwarzaniem danych osobowych zostały umieszczone w odpowiednich umowach. Nowi pracownicy Szpitala przechodzą szkolenia wstępne z zakresu ochrony tych danych.
A.18.1.5	Regulacje dotyczące zabezpieczeń kryptograficznych	*Zabezpieczenie* Szpital nie eksportuje technik kryptograficznych, wobec tego nie dotyczą jej ograniczenia obowiązujące w tym zakresie.

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 bezpieczeństwa informacji	*Zabezpieczenie* W Szpitalu prowadzone są niezależne przeglądy bezpieczeństwa informacji w zaplanowanych odstępach czasu lub wtedy, gdy nastąpiły znaczące zmiany.
A.18.2.2	Zgodność z politykami bezpieczeństwa i standardami	*Zabezpieczenie* Zgodność z politykami bezpieczeństwa i normami badana jest w Szpitalu w sposób systemowy w trakcie przeprowadzanych audytów wewnętrznych realizowanych zgodnie z procedurą „Audity wewnętrzne“.
A.18.2.3	Przegląd zgodności technicznej	*Zabezpieczenie* Sprawdzanie zgodności technicznej realizowane jest w miarę potrzeb przez pracowników zajmujących się utrzymaniem poszczególnych systemów informatycznych.

Rozdzielnik procedury

- Oryginał - Pełnomocnik ds. Zintegrowanego Systemu Zarządzania
  (pozostali mają dostęp do Deklaracji Stosowania w intranecie)

…….
(komórka organizacja - pieczątka)

POTWIERDZENIE ZAPOZNANIA SIĘ PRACOWNIKÓW Z PROCEDURĄ
(odpowiedzialny kierownik komórki organizacyjnej)
Oświadczam, że zapoznałem się z treścią dokumentu i zobowiązuję się do jego stosowania

L.p	Nazwisko i imię	Stanowisko	Data	Podpis

Sporządził :	Sprawdził:	Zatwierdził:

Powiatowe Centrum Zdrowia Sp. z o.o. w Lwówku Śląskim

KARTA ZMIAN

Rodzaj dokumentu: **PROCEDURA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI**	Nr dokumentu: **9/2022/PI**
Tytuł dokumentu: **DEKLARACJA STOSOWANIA**	
Nr wydania: **1**	Data wydania: **30.09.2022**

Lp.	Nr zmiany	Data wprowadzenia zmiany	Strona i punkt objęte zmianą	Krótka charakterystyka zmiany