NR NC-2999/P8

ISO 9001:2015 (PN-EN ISO 9001:2015-10)[1]
ISO 14001:2015 (PN-EN ISO 14001:2015-09)
ISO 45001:2018 (PN-ISO 45001:2018-06)
ISO/IEC 27001:2013 (PN-EN ISO/IEC 27001:2017-06)

[1] Stosowane w treści raportu przywołanie normy ISO, np. ISO 9001 oznacza zarówno normę ISO 9001 jak i polską normę PN-EN ISO 9001.

RAPORT Z AUDITU

1 Wprowadzenie

Audit został przeprowadzony zgodnie z dokumentami Biura Certyfikacji Systemów Zarządzania PRS S.A., w tym m.in.: „Zasadami certyfikacji" (patrz strona internetowa www.prs.pl) oraz procedurami certyfikacji systemu zarządzania PCS-01, na zasadzie próbkowania działań Organizacji związanych z zakresem certyfikacji i zakresem auditu.

Nie stwierdzenie niezgodności z wymaganiami kryteriów auditu nie oznacza, że niezgodności nie występują.

Niniejszy raport zawiera wyniki auditu przeprowadzonego w Organizacji:

Nazwa Organizacji:	**Szpital Powiatowy im. Alfreda Sokołowskiego w Złotowie**	
Adres:	**Szpitalna 28; 77-400 Złotów**	
Przedstawiciel Organizacji:	**Jolanta Konieczna**	
Kryteria auditu:	**ISO 9001; ISO 14001; ISO 45001; ISO/IEC 27001** oraz wymagania Systemu Zarządzania Organizacji; inne wymagania mające zastosowanie w audicie (w tym umowy o certyfikację).	
Data auditu:	**2023-08-21,22**	
Zespół auditorów:	**Jacek Wasiłowski** – Auditor Wiodący PRS **Beata Świerczyńska** – Auditor PRS **Mirosław Żmudziński** – Auditor PRS **Jarosław Płoski** – Auditor PRS	
Opis systemu zarządzania:	**Księga Zintegrowanego Systemu Zarządzania**	Wydanie: **8** Data wydania: **2022-03-11**
	Deklaracja Stosowania:	Wydanie: **3** Data wydania: **2022-03-11**
Plan auditu :	Data opracowania (uzgodnionego): **2023-08-10**	Forma i data uzgodnienia: mail z **2023-08-10**

2 Cele i zakres auditu

2.1 Cele auditu:

Cele auditu są zawarte w planie auditu, stanowiącym załącznik do tego raportu.

2.2 Zakres auditu:

Zakres auditu obejmuje ocenę systemu zarządzania powiązanego z działalnością organizacji określoną w zakresie certyfikacji, zgodnie z powołaniem zespołu auditorów na audit oraz planem auditu.

3 Poufność

Wszelkie informacje uzyskane podczas auditu i wyniki auditu nie będą ujawnione stronie trzeciej bez zgody auditowanej Organizacji. Niniejszy raport z auditu i związane z nim dokumenty mogą być przedstawione Jednostce Akredytującej w trakcie okresowych auditów w Biurze Certyfikacji Systemów Zarządzania PRS S.A. Jednostka Akredytująca jest również zobowiązana do zachowania poufności. Po wydaniu certyfikatu nazwa certyfikowanej organizacji, jej adres i zakres certyfikacji mogą zostać opublikowane.

4 Zakres certyfikacji

4.1. Zakres certyfikowanej działalności

Usługi w zakresie: leczenia szpitalnego, ambulatoryjnej opieki specjalistycznej, podstawowej opieki zdrowotnej, transportu sanitarnego, opieki psychiatrycznej i leczenia uzależnień, diagnostyki laboratoryjnej i obrazowej, diagnostyki endoskopowej, świadczeń pielęgnacyjnych i opiekuńczych, opieki paliatywnej i hospicyjnej, rehabilitacji leczniczej, ratownictwa medycznego Zakres certyfikacji jest zgodny z informacją dotyczącą organizacji.
Wymagania normy ISO 9001:2015, które nie mają zastosowania: 8.3 **Wyłączenia Załącznika A ISO/IEC 27001: A.6.1.5, A.9.4.5, A.14.2.1 i A.14.2.6** **Uzasadnienie:** nie zastosowanie wymagania i wyłączenia zabezpieczeń są uzasadnione specyfiką działania Organizacji.

4.2. Zakres certyfikacji ze względu na lokalizacje (adresy)

Audit był przeprowadzony w siedzibie głównej przy ul. Szpitalnej 28, 77-400 w Złotowie oraz w lokalizacji przywołanej w informacji dotyczącej organizacji, zgodnie z planem auditu (ul. Kolejowa 18, 64-965 Okonek).

5 Ocena systemu zarządzania

Badaniem utrzymywania i doskonalenia systemu zarządzania objęto procesy oraz obszary działalności Organizacji zgodnie z planem auditu. Wyniki oceny z auditu podano poniżej.

5.1. Ocena realizacji powołania zespołu auditorów na audit oraz planu auditu

Warunki wykonania auditu określone w powołaniu zespołu auditorów na audit zostały spełnione. Uzgodniony plan auditu został zrealizowany w pełni. W czasie wykonywania auditu, w planie auditu nie nastąpiły istotne zmiany.

5.2. Ocena zmian wewnętrznych i zewnętrznych w Organizacji, w tym udokumentowanych informacji (i ich nadzoru) systemu zarządzania Organizacji od poprzedniego auditu

W okresie od ostatniego auditu, czasowo został zamknięty Oddział Położniczo Ginekologiczny z Pododdziałem Noworodków oraz dobiega końca generalny remont i rozbudowa ZOL-u. Nie nastąpiły zmiany wynikające z uwarunkowań zewnętrznych. System zarządzania (informacje udokumentowane) jest odpowiedni i przydatny do przyjętego zakresu certyfikacji.

5.3. Ocena wykonania ustaleń z poprzedniego auditu

W poprzednim audicie nie stwierdzono niezgodności. Obserwacje zapisane w ustaleniach z auditu zostały poddane analizie, a na podstawie jej wyników przeprowadzono działania doskonalące.

5.4. Ocena wyników funkcjonowania systemu zarządzania w ostatnim cyklu certyfikacji

Ocena nie ma zastosowania w tym audicie.

5.5. Ocena skuteczności systemu zarządzania, w tym ocena zdolności do realizacji ustanowionej polityki i osiągania celów

System zarządzania Organizacji działa skutecznie, realizuje założone cele oraz zapewnia realizację założonych polityk. Dla zwiększenia skuteczności systemu zarządzania podejmowano liczne działania doskonalące.
Dowodem na to jest osiągnięcie zaplanowanych celów na 2022 rok, podsumowanych w Raporcie z Przeglądu Zarządzania z dnia 2023-08-17.

W okresie sprawozdawczym stwierdzono:
- ilość wypadków i ich rodzaje: 3 wypadki lekkie w 2022 r., w 2023 r. (do czasu auditu): 5 wypadków lekkich;
- ilość zdarzeń potencjalnie wypadkowych: 1 w 2022 r., w 2023 r. (do czasu auditu): 0;
- ilość zarejestrowanych przypadków chorób zawodowych: 0 w 2022 r. i w 2023 r. (do czasu auditu): 0.

Powyższe wyniki świadczą o potencjale do doskonalenia SZBHP.

5.6. Ocena zdolności systemu zarządzania Organizacji do zapewnienia spełnienia mających zastosowanie w jej działalności wymagań przepisów prawnych, regulacyjnych i umów

System zarządzania Organizacji zapewnia zdolność do spełnienia przez Organizację mających zastosowanie wymagań, przepisów prawnych, regulacyjnych i umów.

W zakresie BHP:
- nie stwierdzono poważnych incydentów wymagających zgłoszenia do PRS, od ostatniego auditu;
- nie stwierdzono naruszeń prawa w 2022 r.;
- nie stwierdzono naruszeń prawa w 2023 r. (do czasu auditu).

5.7. Ocena poziomu integracji systemu zarządzania organizacji

Określony poziom integracji systemu zarządzania organizacji w ramach przeglądu wniosku jest określony właściwie.

5.8. Ocena i ustalenia z auditu na podstawie umowy o certyfikację

Umowa o certyfikację jest realizowana. Znaki certyfikacji są stosowane zgodnie z umową, np. na listownikach. Organizacja przekazuje do Biura Certyfikacji Systemów Zarządzania PRS S.A. ważne informacje dotyczące zmian w systemie zarządzania.

5.9. Ocena zgodności z wymaganiami

Do oceny zastosowano następujące symbole:

O - wymagania wyłączone z auditu (zgodnie z planem auditu).
W - wyłączenie wymagań (wskazane w punkcie 4 raportu).
+ - wymagania spełnione (może wystąpić obserwacja).
— - wymaganie niespełnione (występuje niezgodność).
Numer niezgodności/obserwacji – wg ustaleń z auditu.

5.9.1 Ocena i ustalenia z auditu wg wymagań normy ISO 9001

Nr punktu normy	WYMAGANIA NORMY ISO 9001	Ocena	Numer niezgodności/obserwacji, uwagi
4	**Kontekst organizacji**		
4.1	Zrozumienie organizacji i jej kontekstu	+	
4.2	Zrozumienie potrzeb i oczekiwań stron zainteresowanych	+	
4.3	Określenie zakresu systemu zarządzania jakością	+	
4.4	System zarządzania jakością i jego procesy	+	
5	**Przywództwo**		
5.1	Przywództwo i zaangażowanie	+	
5.2	Polityka	+	
5.3	Role, odpowiedzialność i uprawnienia w organizacji	+	
6	**Planowanie**		
6.1	Działania odnoszące się do ryzyk i szans	+	

RAPORT Z AUDITU

Nr punktu normy	WYMAGANIA NORMY ISO 9001	Ocena	Numer niezgodności/obserwacji, uwagi
6.2	Cele jakościowe i planowanie ich osiągnięcia	+	
6.3	Planowanie zmian	+	
7	**Wsparcie**		
7.1	Zasoby	+	O3
7.2	Kompetencje	+	
7.3	Świadomość	+	
7.4	Komunikacja	+	
7.5	Udokumentowane Informacje	+	
8	**Działania operacyjne**		
8.1	Planowanie i nadzór nad działaniami operacyjnymi	+	
8.2	Wymagania dotyczące wyrobów i usług	+	
8.3	Projektowanie i rozwój wyrobów i usług	W	
8.4	Nadzór nad procesami, wyrobami i usługami dostarczanymi z zewnątrz	+	
8.5	Produkcja i dostarczanie usługi	+	
8.6	Zwolnienie wyrobów i usług	+	
8.7	Nadzór nad niezgodnymi wyjściami	+	
9	**Ocena efektów działania**		
9.1	Monitorowanie, pomiary, analiza i ocena	+	
9.2	Audit wewnętrzny	+	
9.3	Przegląd zarządzania	+	
10	**Doskonalenie**		
10.1	Postanowienia ogólne	+	
10.2	Niezgodności i działania korygujące	+	
10.3	Ciągłe doskonalenie	+	

5.9.2 Ocena i ustalenia z auditu wg wymagań normy ISO 14001

Nr punktu normy	WYMAGANIA NORMY ISO 14001	Ocena	Numer niezgodności/obserwacji, uwagi
4	**Kontekst organizacji**		
4.1	Zrozumienie organizacji i jej kontekstu	+	
4.2	Zrozumienie potrzeb i oczekiwań stron zainteresowanych	+	
4.3	Określenie zakresu systemu zarządzania środowiskowego	+	
4.4	System zarządzania środowiskowego	+	
5	**Przywództwo**		
5.1	Przywództwo i zaangażowanie	+	
5.2	Polityka środowiskowa	+	
5.3	Role, odpowiedzialności i uprawnienia w organizacji	+	
6	**Planowanie**		
6.1	Działania odnoszące się do ryzyk i szans	+	

RAPORT Z AUDITU

Nr punktu normy	WYMAGANIA NORMY ISO 14001	Ocena	Numer niezgodności/obserwacji, uwagi
6.2	Cele środowiskowe i planowanie ich osiągnięcia	+	
7	**Wsparcie**		
7.1	Zasoby	+	
7.2	Kompetencje	+	
7.3	Świadomość	+	
7.4	Komunikacja	+	
7.5	Udokumentowane informacje	+	**O2**
8	**Działania operacyjne**		
8.1	Planowanie i nadzór nad działaniami operacyjnymi	+	
8.2	Gotowość i reagowanie na sytuacje awaryjne	+	
9	**Ocena efektów działania**		
9.1	Monitorowanie, pomiary, analiza i ocena	+	
9.2	Audit wewnętrzny	+	
9.3	Przegląd zarządzania	+	
10	**Doskonalenie**		
10.1	Postanowienia ogólne	+	
10.2	Niezgodności i działania korygujące	+	
10.3	Ciągłe doskonalenie	+	

5.9.3 Ocena i ustalenia z auditu wg wymagań normy ISO 45001

Nr punktu normy	WYMAGANIA NORMY ISO 45001	Ocena	Numer niezgodności/obserwacji, uwagi
4	**Kontekst organizacji**		
4.1	Zrozumienie organizacji i jej kontekstu	+	
4.2	Zrozumienie potrzeb i oczekiwań pracowników i innych stron zainteresowanych	+	
4.3	Określenie zakresu systemu zarządzania BHP	+	
4.4	System zarządzania BHP	+	
5	**Przywództwo i uczestnictwo pracowników**		
5.1	Przywództwo i zaangażowanie	+	
5.2	Polityka BHP	+	
5.3	Role, odpowiedzialności i uprawnienia w organizacji	+	
5.4	Konsultacje i uczestnictwo pracowników	+	
6	**Planowanie**		
6.1	Działania odnoszące się do ryzyk i szans	+	**06**
6.2	Cele BHP i planowanie ich osiągnięcia	+	
7	**Wsparcie**		
7.1	Zasoby	+	

RAPORT Z AUDITU

Nr punktu normy	WYMAGANIA NORMY ISO 45001	Ocena	Numer niezgodności/obserwacji, uwagi
7.2	Kompetencje	+	
7.3	Świadomość	+	
7.4	Informacja i Komunikacja	+	
7.5	Udokumentowane informacje	+	O5
8	**Działania operacyjne**		
8.1	Planowanie i nadzór nad działaniami operacyjnymi	+	
8.2	Gotowość i reagowanie awaryjne	+	
9	**Ocena efektów działania**		
9.1	Monitorowanie, pomiary, analiza i ocena	+	
9.2	Audit wewnętrzny	+	
9.3	Przegląd zarządzania	+	
10	**Doskonalenie**		
10.1	Postanowienia ogólne	+	
10.2	Incydent, niezgodności i działania korygujące	+	
10.3	Ciągłe doskonalenie	+	

5.9.4 Ocena i ustalenia z auditu wg wymagań normy ISO/IEC 27001

Nr punktu normy	WYMAGANIA NORMY ISO/IEC 27001	Ocena	Numer niezgodności/obserwacji, uwagi
4	**Kontekst Organizacji**		
4.1	Zrozumienie organizacji i jej kontekstu	+	
4.2	Zrozumienie potrzeb i oczekiwań stron zainteresowanych	+	
4.3	Określenie zakresu SZBI	+	
4.4	System zarządzania bezpieczeństwem informacji	+	
5	**Przywództwo**		
5.1	Przywództwo i zaangażowanie	+	
5.2	Polityka	+	
5.3	Role, odpowiedzialność i uprawnienia	+	
6	**Planowanie**		
6.1	Działania odnoszące się do ryzyk i szans	+	
6.2	Cele bezpieczeństwa informacji i planowanie ich osiągnięcia	+	
7	**Wsparcie**		
7.1	Zasoby	+	
7.2	Kompetencje	+	
7.3	Uświadamianie	+	
7.4	Komunikacja	+	
7.5	Udokumentowane informacje	+	

RAPORT Z AUDITU

Nr punktu normy	WYMAGANIA NORMY ISO/IEC 27001	Ocena	Numer niezgodności/obserwacji, uwagi
8	**Eksploatacja**		
8.1	Planowanie i nadzór nad działaniami operacyjnymi	+	
8.2	Szacowanie ryzyka w bezpieczeństwie informacji	+	
8.3	Postępowanie z ryzykiem w bezpieczeństwie informacji	+	
9	**Ocena wyników działalności**		
9.1	Monitorowanie, pomiary, analiza i ocena	+	
9.2	Audyt wewnętrzny	+	
9.3	Przegląd zarządzania	+	
10	**Doskonalenie**		
10.1	Niezgodność i działania korygujące	+	
10.2	Ciągłe doskonalenie	+	

Załącznik A do ISO/IEC 27001: Zabezpieczenia

Nr zabezpieczenia	Nazwa zabezpieczenia	Ocena	Numer niezgodności/obserwacji, uwagi
A.5	**Polityki bezpieczeństwa informacji**		
A.5.1	**Kierunki bezpieczeństwa informacji określane przez kierownictwo**		
A.5.1.1	Polityki bezpieczeństwa informacji	+	
A.5.1.2	Przegląd polityk bezpieczeństwa informacji	+	
A.6	**Organizacja bezpieczeństwa informacji**		
A.6.1	**Organizacja wewnętrzna**		
A.6.1.1	Role i odpowiedzialność za bezpieczeństwo informacji	+	
A.6.1.2	Rozdzielanie obowiązków	+	
A.6.1.3	Kontakty z organami władzy	+	
A.6.1.4	Kontakty z grupami zainteresowanych specjalistów	+	
A.6.1.5	Bezpieczeństwo informacji w zarządzaniu projektami	W	
A.6.2	**Urządzenia mobilne i telepraca**		
A.6.2.1	Polityka stosowania urządzeń mobilnych	+	
A.6.2.2	Telepraca	+	
A.7	**Bezpieczeństwo zasobów ludzkich**		
A.7.1	**Przed zatrudnieniem**		
A.7.1.1	Postępowanie sprawdzające	+	
A.7.1.2	Warunki zatrudnienia	+	
A.7.2	**Podczas zatrudnienia**		
A.7.2.1	Odpowiedzialność kierownictwa	+	
A.7.2.2	Uświadamianie, kształcenie i szkolenia z zakresu BI	+	**O1**
A.7.2.3	Postępowanie dyscyplinarne	+	

RAPORT Z AUDITU

Nr zabezpieczenia	Nazwa zabezpieczenia	Ocena	Numer niezgodności/obserwacji, uwagi
A.7.3	**Zakończenie i zmiana zatrudnienia**		
A.7.3.1	Zakończenie zatrudnienia lub zmiana zakresu obowiązków	+	
A.8	**Zarządzanie aktywami**		
A.8.1	**Odpowiedzialność za aktywa**		
A.8.1.1	Inwentaryzacja aktywów	+	
A.8.1.2	Własność aktywów	+	
A.8.1.3	Akceptowalne użycie aktywów	+	
A.8.1.4	Zwrot aktywów	+	
A.8.2	**Klasyfikacja informacji**		
A.8.2.1	Klasyfikowanie informacji	+	
A.8.2.2	Oznaczanie informacji	+	O4
A.8.2.3	Postępowanie z aktywami	+	
A.8.3	**Postępowanie z nośnikami**		
A.8.3.1	Zarządzanie nośnikami wymiennymi	+	
A.8.3.2	Wycofywanie nośników	+	
A.8.3.3	Przekazywanie nośników	+	
A.9	**Kontrola dostępu**		
A.9.1	**Wymagania biznesowe wobec kontroli dostępu**		
A.9.1.1	Polityka kontroli dostępu	+	
A.9.1.2	Dostęp do sieci i usług sieciowych	+	
A.9.2	**Zarządzanie dostępem użytkowników**		
A.9.2.1	Rejestrowanie i wyrejestrowanie użytkowników	+	
A.9.2.2	Przydzielenie dostępu użytkownikom	+	
A.9.2.3	Zarządzanie prawami uprzywilejowanego dostępu	+	
A.9.2.4	Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników	+	
A.9.2.5	Przegląd praw dostępu użytkowników	+	
A.9.2.6	Odbieranie lub dostosowywanie praw dostępu	+	
A.9.3	**Odpowiedzialność użytkowników**		
A.9.3.1	Stosowanie poufnych informacji uwierzytelniających	+	
A.9.4	**Kontrola dostępu do systemów i aplikacji**		
A.9.4.1	Ograniczanie dostępu do informacji	+	
A.9.4.2	Procedury bezpiecznego logowania	+	
A.9.4.3	System zarządzania hasłami	+	
A.9.4.4	Użycie uprzywilejowanych programów narzędziowych	+	
A.9.4.5	Kontrola dostępu do kodu źródłowego programu	W	
A.10	**Kryptografia**		
A.10.1	**Zabezpieczenia kryptograficzne**		
A.10.1.1	Polityka stosowania zabezpieczeń kryptograficznych	+	

RAPORT Z AUDITU

Nr zabezpieczenia	Nazwa zabezpieczenia	Ocena	Numer niezgodności/obserwacji, uwagi
A.10.1.2	Zarządzanie kluczami	+	
A.11	**Bezpieczeństwo fizyczne i środowiskowe**		
A.11.1	**Obszary bezpieczne**		
A.11.1.1	Fizyczna granica obszaru bezpiecznego	+	
A.11.1.2	Fizyczne zabezpieczenie wejść	+	
A.11.1.3	Zabezpieczenie biur, pomieszczeń i obiektów	+	
A.11.1.4	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	+	
A.11.1.5	Praca w obszarach bezpiecznych	+	
A.11.1.6	Obszary dostaw i załadunku	+	
A.11.2	**Sprzęt**		
A.11.2.1	Lokalizacja i ochrona sprzętu	+	
A.11.2.2	Systemy wspomagające	+	
A.11.2.3	Bezpieczeństwo okablowania	+	
A.11.2.4	Konserwacja sprzętu	+	
A.11.2.5	Wynoszenie aktywów	+	
A.11.2.6	Bezpieczeństwo sprzętu i aktywów poza siedzibą	+	
A.11.2.7	Bezpieczne zbywanie lub przekazywanie do ponownego użycia	+	
A.11.2.8	Pozostawianie sprzętu użytkownika bez opieki	+	
A.11.2.9	Polityka czystego biurka i czystego ekranu	+	
A.12	**Bezpieczna eksploatacja**		
A.12.1	**Procedury eksploatacyjne i odpowiedzialność**		
A.12.1.1	Dokumentowanie procedur eksploatacyjnych	+	
A.12.1.2	Zarządzanie zmianami	+	
A.12.1.3	Zarządzanie pojemnością	+	
A.12.1.4	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	+	
A.12.2	**Ochrona przed złośliwym oprogramowaniem**		
A.12.2.1	Zabezpieczenie przed złośliwym oprogramowaniem	+	
A.12.3	**Kopie zapasowe**		
A.12.3.1	Zapasowe kopie informacji	+	
A.12.4	**Rejestrowanie zdarzeń i monitorowanie**		
A.12.4.1	Rejestrowanie zdarzeń	+	
A.12.4.2	Ochrona informacji w dziennikach zdarzeń	+	
A.12.4.3	Rejestrowanie działań administratorów i operatorów	+	
A.12.4.4	Synchronizacja zegarów	+	
A.12.5	**Nadzór na oprogramowaniem produkcyjnym**		
A.12.5.1	Instalacja oprogramowania w systemach produkcyjnych	+	
A.12.6	**Zarządzanie podatnościami technicznymi**		
A.12.6.1	Zarządzanie podatnościami technicznymi	+	

RAPORT Z AUDITU

Nr zabezpieczenia	Nazwa zabezpieczenia	Ocena	Numer niezgodności/obserwacji, uwagi
A.12.6.2	Ograniczenia w instalowaniu oprogramowania	+	
A.12.7	**Rozważania dotyczące audytów systemów informacyjnych**		
A.12.7.1	Zabezpieczenia audytu systemów informacyjnych	+	
A.13	**Bezpieczeństwo komunikacji**		
A.13.1	**Zarządzanie bezpieczeństwem sieci**		
A.13.1.1	Zabezpieczenia sieciowe	+	
A.13.1.2	Bezpieczeństwo usług sieciowych	+	
A.13.1.3	Rozdzielanie sieci	+	
A.13.2	**Przesyłanie informacji**		
A.13.2.1	Polityki i procedury przesyłania informacji	+	
A.13.2.2	Porozumienia dotyczące przesyłania informacji	+	
A.13.2.3	Wiadomości elektroniczne	+	
A.13.2.4	Umowy o zachowaniu poufności	+	
A.14	**Pozyskiwanie, rozwój i utrzymanie systemów**		
A.14.1	**Wymagania związane z bezpieczeństwa systemów informacyjnych**		
A.14.1.1	Analiza i specyfikacja wymagań bezpieczeństwa informacji	+	
A.14.1.2	Zabezpieczania usług aplikacyjnych w sieciach publicznych	+	
A.14.1.3	Ochrona transakcji usług aplikacyjnych	+	
A.14.2	**Bezpieczeństwo w procesach rozwoju i wsparcia**		
A.14.2.1	Polityka bezpieczeństwa prac rozwojowych	W	
A.14.2.2	Procedury kontroli zmian w systemach	+	
A.14.2.3	Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	+	
A.14.2.4	Ograniczenia dotyczące zmian w pakietach oprogramowania	+	
A.14.2.5	Zasady projektowania bezpiecznych systemów	+	
A.14.2.6	Bezpieczne środowisko rozwojowe	W	
A.14.2.7	Prace rozwojowe zlecane pomiotom zewnętrznym	+	
A.14.2.8	Testowanie bezpieczeństwa systemów	+	
A.14.2.9	Testy akceptacyjne systemów	+	
A.14.3	**Dane testowe**		
A.14.3.1	Ochrona danych testowych	+	
A.15	**Relacje z dostawcami**		
A.15.1	**Bezpieczeństwo informacji w relacjach z dostawcami**		
A.15.1.1	Polityka bezpieczeństwa informacji w relacjach z dostawcami	+	
A.15.1.2	Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami	+	
A.15.1.3	Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych	+	
A.15.2	**Zarządzanie usługami świadczonymi przez dostawców**		
A.15.2.1	Monitorowanie i przegląd usług świadczonych zez dostawców.	+	
A.15.2.2	Zarządzanie zmianami w usługach świadczonych przez dostawców	+	

Nr zabezpieczenia	Nazwa zabezpieczenia	Ocena	Numer niezgodności/obserwacji, uwagi
A.16	**Zarządzanie incydentami związanymi z bezpieczeństwem informacji**		
A.16.1	**Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami**		
A.16.1.1	Odpowiedzialność i procedury	+	
A.16.1.2	Zgłaszanie zdarzeń związanych z BI	+	
A.16.1.3	Zgłaszanie słabości związanych z BI	+	
A.16.1.4	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z BI	+	
A.16.1.5	Reagowanie na incydenty związane z BI	+	
A.16.1.6	Wyciąganie wniosków z incydentów związanych z BI	+	
A.16.1.7	Gromadzenie materiału dowodowego	+	
A.17	**Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania**		
A.17.1	**Ciągłość bezpieczeństwa informacji**		
A.17.1.1	Planowanie ciągłości BI	+	
A.17.1.2	Wdrażanie ciągłości BI	+	
A.17.1.3	Weryfikowanie, przegląd i ocena ciągłości BI	+	
A.17.2	**Nadmiarowość**		
A.17.2.1	Dostępność środków przetwarzania informacji	+	
A.18	**Zgodność**		
A.18.1	**Zgodność z wymaganiami prawnymi i umownymi**		
A.18.1.1	Określenie stosownych wymagań prawnych i umownych	+	
A.18.1.2	Prawa własności intelektualnej	+	
A.18.1.3	Ochrona zapisów	+	
A.18.1.4	Prywatność i ochrona danych identyfikujących osobę	+	
A.18.1.5	Regulacje dotyczące zabezpieczeń kryptograficznych	+	
A.18.2	**Przeglądy bezpieczeństwa informacji**		
A.18.2.1	Niezależny przegląd BI	+	
A.18.2.2	Zgodność z politykami bezpieczeństwa i standardami	+	
A.18.2.3	Sprawdzanie zgodności technicznej	+	

6 Wnioski i rekomendacje

6.1. Wnioski ogólne:

Audit dostarczył dowodów, że System Zarządzania Organizacji jest utrzymywany i doskonalony, zgodnie z wymaganiami norm odniesienia oraz innymi mającymi zastosowanie wymaganiami. W audicie nie stwierdzono niezgodności. Zapisane w ustaleniach z auditu obserwacje wskazują potencjalne obszary do doskonalenia systemu zarządzania.

6.2. Silne strony Organizacji:

- Szeroki zakres świadczonych usług medycznych
- Rozwój infrastruktury zapewniający lepszą obsługę pacjentów i poprawę jakości usług medycznych
- Bieżące przeglądy i aktualizacja ocen ryzyka zawodowego.

- Innowacyjne metody leczenia

6.3. Wnioski dotyczące przebiegu auditu

W trakcie auditu nie wystąpiły żadne problemy związane z przebiegiem auditu. Organizacja nie zgłosiła żadnych rozbieżnych z auditorami opinii, które wymagałyby rozstrzygnięcia przez Biuro Certyfikacji Systemów Zarządzania.

6.4. Wnioski dotyczące potwierdzenia, że cele auditu zostały spełnione

Przebieg auditu oraz dowody uzyskane w trakcie auditu potwierdzają, że cele auditu zostały osiągnięte. W audicie nie stosowano technologii informacyjno-komunikacyjnych (ICT).

6.5. Wnioski i ustalenia szczegółowe dotyczące ISO 9001:

Najwyższe kierownictwo przyjęło i zapewniło realizację polityki jakości. Procesy zostały zidentyfikowane, określono wzajemne powiązania pomiędzy procesami i metody zapewniające skuteczne nadzorowanie procesów. Określono kryteria i metody dla zapewnienia skuteczności przebiegu i nadzorowania procesów. Dostępne są zasoby i informacje niezbędne do wspomagania przebiegu i monitorowania procesów. Procesy są monitorowane, mierzone i analizowane. Wdrażane są działania do ciągłego doskonalenia procesów i systemu zarządzania.

6.6. Wnioski i ustalenia szczegółowe dotyczące ISO 14001:

Najwyższe kierownictwo przyjęło i zapewniło realizację polityki środowiskowej. Zidentyfikowano i oceniono występujące w organizacji aspekty środowiskowe, na które organizacja może mieć wpływ, z uwzględnieniem perspektywy cyklu życia oraz określono zagrożenia i możliwości związane z tymi aspektami środowiskowymi. Ustalono zobowiązania do zachowywania zgodności z wymaganiami dotyczącymi aspektów środowiskowych i utrzymuje się udokumentowaną informację dotyczącą przyjętych zobowiązań do zgodności z wymaganiami. Organizacja monitoruje i ocenia efekty swoich działań mogących mieć wpływ na środowisko. Cele środowiskowe są planowane, z uwzględnieniem znaczących aspektów środowiskowych oraz związanych z nimi zobowiązań do zgodności z wymaganiami, a także zagrożeń i możliwości, monitorowane i przedstawiono dowody ich osiągania. Organizacja rozpatruje powiązanie działań zmierzających do osiągania celów środowiskowych z jej procesami biznesowymi. Najwyższe kierownictwo określiło odpowiedzialności za realizację przyjętej polityki środowiskowej i doskonalenie ustanowionego systemu zarządzania.

6.7. Wnioski i ustalenia szczegółowe dotyczące ISO 45001:

Najwyższe kierownictwo przyjęło i zapewniło realizację polityki bezpieczeństwa i higieny pracy. Zidentyfikowano i oceniono występujące w organizacji zagrożenia BHP. Organizacja dokonała wdrożenia takich elementów systemu zarządzania BHP jak: działania odnoszące się do ryzyk i szans, planowanie i nadzór operacyjny, postępowanie z incydentami oraz inne działania. Zapewniono odpowiedzialność pracodawcy, kadry kierowniczej i pracowników za BHP. Określono cele BHP i programy osiągania bezpiecznych warunków pracy i przedstawiono dowody ich realizacji. Ustanowiony system zarządzania bezpieczeństwem i higieną pracy podlega doskonaleniu.

6.8. Wnioski i ustalenia szczegółowe dotyczące ISO/IEC 27001:

Najwyższe kierownictwo przyjęło i zapewniło realizację polityki bezpieczeństwa informacji. Zidentyfikowano aktywa i oceniono występujące w organizacji zagrożenia. Ustalono występujące w organizacji ryzyka związane z bezpieczeństwem informacji oraz określono sposób postępowania z ryzykiem. Określono deklarację stosowania zabezpieczeń dla ograniczenia ryzyk oraz zapewnienia działania organizacji zgodnego z obowiązującym prawem i innymi zobowiązaniami organizacji, dla zapewnienia bezpieczeństwa działania organizacji. Ustanowiony system zarządzania bezpieczeństwem informacji podlega doskonaleniu.

6.9. Rekomendacja podstawowa:

Utrzymać ważność certyfikatu: - bo nie stwierdzono niezgodności	✓

6.10. Rekomendacje uzupełniające:

6.10.1 W obszarze Systemu Zarzadzania Bezpieczeństwem Informacji ponowna certyfikacja systemu w 2024 r., po 2024-04-30 będzie możliwa tylko na zgodność z wymaganiami normy ISO/IEC 27001:2022.

6.10.2 Zaleca się Organizacji przeanalizowanie ryzyk związanych ze stwierdzonymi obserwacjami oraz na jej podstawie zaproponowanie i realizację działań doskonalących.

6.10.3 Organizacja jest zobowiązana do informowania Biura Certyfikacji Systemów Zarządzania PRS S.A. o znaczących zmianach w systemie zarządzania, w szczególności do przesyłania aktualnych dokumentów systemu zarządzania (np. Księgi ZSZ).

7 Załączniki

Program auditów	Form. 3/PCS-01/QMS (plik doc),
Plan auditu	Form. 4/PCS-01/QMS (plik pdf),
Kwestionariusz auditu	Form. 5/PCS-01/QMS (plik pdf - 4 pliki),
Kwestionariusz z auditu ISMS	Form. 1/PCS/ISMS (plik pdf - 3 pliki),
Załącznik 1 do kwestionariusza auditu	Zał. 1 Form. 5/PCS-01/QMS (plik pdf),
Ustalenia z auditu	Form. 6/PCS-01/QMS (plik pdf i kopia przesłana Organizacji w trakcie auditu).

8 Rozdzielnik

Raport z auditu otrzymuje Organizacja (plik w formacie pdf bez kwestionariusza auditu oraz programu auditów). Raport jest własnością Biura Certyfikacji Systemów Zarządzania PRS S.A.

Auditor wiodący[2]:	Data:
Jacek Wasiłowski	**2023-08-28**

Uwagi:

1 *Do niniejszego raportu i/lub przebiegu auditu przysługuje Organizacji prawo zgłaszania uwag. Brak zgłoszenia uwag, w terminie 10 dni od otrzymania raportu, uznane będzie za przyjęcie treści raportu.*

2 *Sformułowania w rekomendacji typu „wydać certyfikat" są równorzędne pojęciu „udzielić certyfikacji".*

[2] Dokument jest autoryzowany przez auditora wiodącego w formie wpisu imienia i nazwiska