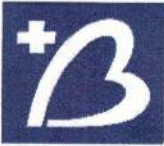
	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 1 z 31 PR1.3_SD1_w1

Spis treści:

- 1 Standard Zarządzania Systemem Informatycznym – Instrukcja Zarządzania Systemem Informatycznym **str. 2**
- 2 Standard Zarządzania Systemem Informatycznym – Polityka Bezpieczeństwa **str. 19**

Opracował: Lider Procesu	Sprawdził: Pełnomocnik ds. SZJ	Zatwierdził: Dyrektor
Data: <i>09.05.2016</i>	Data: <i>16.05.16</i>	Data: 17 MAJ 2016 DYREKTOR
Podpis: <i>KIEROWNIK Działu Informatyki</i> <i>mgr inż. Krzysztof Nowakowski</i>	Podpis: <i>Pełnomocnik ds. Zintegrowanego Systemu Zarządzania</i> <i>mgr Renata Łojewska</i>	Podpis: <i>Dyrektor ds. Administracyjno-Technicznych Szpitala Uniwersyteckiego Nr 2 im. dr Jana Biegasa w Bydgoszczy</i> <i>mgr Leszek Kowalik</i>


	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 2 z 31 PR1.3_SD1_w1

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Szpitala Uniwersyteckiego Nr 2 im. dr. Jana Biziela w Bydgoszczy

Spis treści:

I	Definicje.	str. 3
II	Procedury nadawania i zmiany uprawnień do przetwarzania danych w systemach informatycznych.	str. 4
III	Zasady posługiwania się hasłami.	str. 4
IV	Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.	str. 4
V	Procedury tworzenia kopii bezpieczeństwa.	str. 5
VI	Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków.	str. 5
VII	Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi.	str. 6
VIII	Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych.	str. 7
IX	Sposób postępowania w sytuacji naruszenia ochrony danych osobowych.	str. 7
X	Procedury wykonywania przeglądów i konserwacji systemu.	str. 7
XI	Sieć LAN oraz dostęp do Bibliotek.	str. 8
XII	Połączenie do sieci Internet.	str. 9
XIII	Procedury korzystania z komputerów przenośnych.	str. 9
XIV	Procedura korzystania z poczty wewnętrznej i Intranetu.	str. 10
XV	Procedura dostępu zdalnego do sieci Szpitala.	str. 11
XVI	Odpowiedzialność.	str. 12
XVII	Załączniki.	str. 14

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 3 z 31 PR1.3_SD1_w1


Podstawa prawna:

- Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005r. w sprawie wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2005 Nr 171 poz. 1433 z dnia 8 września 2005r.)
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 Nr 100, poz. 1024)
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 Nr 101, poz. 926 z późn. zm.)

I. Definicje.

Ileokroć w niniejszym dokumencie jest mowa o:

- Szpitalu** - należy przez to rozumieć Szpital Uniwersytecki Nr 2 im. dr. J.Biziela w Bydgoszczy,
- Administratorze Bezpieczeństwa Informacji** - należy przez to rozumieć pracownika szpitala wyznaczonego do nadzorowania przestrzegania zasad ochrony danych osobowych ustanowionego zgodnie z Zarządzeniem Dyrektora Szpitala Uniwersyteckiego Nr 2.im.dr.J.Biziela,
- Administratorze Systemu Informatycznego** - należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu teleinformatycznego szpitala oraz stosowanie technicznych i organizacyjnych środków ochrony,
- użytkownika systemu** - należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym Szpitala. Użytkownikiem może być pracownik Szpitala, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w Szpitalu lub wolontariusz,
- sieci lokalnej** - należy przez to rozumieć połączenie systemów informatycznych Szpitala wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,
- sieci rozległej** - należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, póź. 852, z późn. zm.)

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 4 z 31 PR1.3_SD1_w1

II. Procedury nadawania i zmiany uprawnień do przetwarzania danych w systemach informatycznych.

Procedury nadawania i zmiany uprawnień do przetwarzania danych w systemach informatycznych zostały opisane w Polityce Nadawania Uprawnień w Systemie Informatycznym.

Dokument znajduje się w PISZ pod linkiem: <http://pisz/index.php?it=56>

III. Zasady posługiwania się hasłami.

Zasady posługiwania się hasłami zostały opisane w Polityce Nadawania Uprawnień w Systemie Informatycznym.

Dokument znajduje się w PISZ pod linkiem: <http://pisz/index.php?it=56>


Administrator Systemu Informatycznego prowadzi REJESTR UŻYTKOWNIKÓW I UPRAWNIENÍ W SYSTEMIE INFORMATYCZNYM zgodnie z **Załącznikiem Nr 1**

IV. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

1. Przed rozpoczęciem pracy w systemie komputerowym należy zameldować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przy opuszczeniu stanowiska pracy należy wykonać opcję wymeldowania z systemu (zablokowania dostępu), lub jeżeli taka możliwość nie istnieje wyjść z programu.
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wymeldowania z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wymeldować się z sieci komputerowej.
5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.
6. Nie używaj komputerów przenośnych do celów prywatnych oraz nie wypożyczaj ich innym osobom nawet w obrębie organizacji.
7. Praca poza biurem rodzi duże ryzyko utraty danych, a także zwiększa ekspozycję prawdopodobieństwa utraty zasobów teleinformatycznych w drodze kradzieży lub zagubienia.

- Praca w środkach lokomocji publicznej z wykorzystaniem zasobów teleinformatycznych

1. Pamiętaj, aby do minimum ograniczyć pracę z wrażliwymi danymi w środkach lokomocji publicznej, w przypadku, gdy zajdzie taka konieczność, zwróć uwagę czy osoby postronne nie mają możliwości wglądu w ekran twojego pulpitu.
2. Nigdy nie zostawiaj żadnego urządzenia bez opieki

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 5 z 31 PR1.3_SD1_w1

- Podróże samochodem służbowym

1. Pamiętaj, aby w trakcie podróży samochodem służbowym, nigdy nie pozostawiać w samochodzie żadnych dokumentów ani urządzeń teleinformatycznych Szpitala,
2. Pamiętaj, aby nie trzymać komputera w osobowej części samochodu – zawsze zamykaj komputer w bagażniku samochodu.

V. Procedury tworzenia kopii bezpieczeństwa.


Procedura tworzenia kopii bezpieczeństwa została opisana w Polityce Tworzenia Kopii Zapasowych.

Dokument znajduje się w PISZ pod linkiem: <http://pisz/index.php?it=56>

VI. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków.

A. Elektroniczne nośniki informacji.

1. Do nośników informacji zaliczamy dyski twarde, płyty CD, pamięci przenośne itp.
2. Użytkownicy stacji roboczych co do zasady posiadają zablokowane porty USB oraz napędy CD ROM. W przypadku specjalnych uprawnień – (pisemnie) istnieje możliwość udostępnienia portów USB oraz napędów CDROM.
3. Nośniki danych podlegają rejestracji (wykaz nośników znajduje się pod linkiem http://pisz/ewidencja/ewidencja_pendrive.php) . W ewidencji rejestrowane są następujące informacje:
 - Nazwa urządzenia
 - Numer identyfikacyjny
 - Data otrzymania
4. Każdy nośnik powinien posiadać trwale umocowany nr nośnika. Stosuję się przyjęte w Polityce metody szyfrowania nośników.
5. Przekazanie nośników typu: dyski twarde, pamięci przenośne itp., do użytku przez pracowników Szpitala odbywa się na podstawie Protokołu Zdawczo-Odbiorczego.
6. Dane wg polityki klasyfikacji informacji w postaci elektronicznej – zapisane na dyskietkach, dyskach magnetoptycznych, pamięć przenośna USB czy dyskach twardych nie są wynoszone poza siedzibę Szpitala.
7. Wymienne elektroniczne nośniki informacji są przechowywane w pomieszczeniach służbowych.
8. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub kasetkach.
9. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
10. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 6 z 31 PR1.3_SD1_w1

otrzymywania

danych osobowych pozbawia się wcześniej zapisu tych danych.


11. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia sieje pod nadzorem osoby upoważnionej.
12. W sytuacji udostępniania nośnika lub przekazywania go w posiadanie innej uprawnionej osobie, Użytkownik winien zweryfikować dane zapisane na nośniku i usunąć z niego wszystkie Informacje inne niż te, które zamierza udostępnić osobie, której przekazuje nośnik.
13. Nie pozostawiaj bez opieki służbowego telefonu komórkowego
14. Nie używaj prywatnego komputera czy telefonu do gromadzenia danych Firmy

B. Wydruki.

1. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
2. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.
3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.
4. W bazie danych gromadzone są informacje o loginie i czasie wykonania wydruku Karty Informacyjnej oraz Historii Choroby.

VII. Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi.

1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora.
2. Każdy e-mail wpływający do Szpitala musi być sprawdzony pod kątem występowania wirusów przez bramę antywirusową.
3. Definicje wzorców wirusów aktualizowane są zgodnie z polityką konsoli zarządzającej.
4. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
6. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: PR 1.3	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 7 z 31 PR1.3_SD1_w1

7. Administrator Systemu Informatycznego przeprowadza analizę zagrożeń wirusowych na wszystkich komputerach – minimum raz na dobę poprzez konsolę zarządzającą.
8. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika nośniki.

VIII. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych.

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.
2. Udostępnienie danych osobowych, w jakiegokolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia Administratora Bezpieczeństwa Informacji.
3. Kierownicy komórek organizacyjnych prowadzą rejestry udostępnionych danych osobowych zawierające co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucję dla której dane udostępniono.
4. Aplikacje wykorzystywane do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych. Zakres informacji powinien obejmować, co najmniej: dane odbiorcy, datę wydania, zakres udostępnionych danych.

IX. Sposób postępowania w sytuacji naruszenia ochrony danych osobowych.


Sposób postępowania w sytuacji stwierdzenia naruszenia ochrony danych określa **Załącznik Nr 2** do niniejszego dokumentu.

X. Procedury wykonywania przeglądów i konserwacji systemu.

A. Przeglądy i konserwacja urządzeń.

1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonym przez producenta sprzętu.
2. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Systemu Informatycznego.

B. Przegląd programów i narzędzi programowych.

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 8 z 31 PR1.3_SD1_w1

1. Konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.
2. Administrator Bezpieczeństwa Systemu Informatycznego zobowiązany jest uaktywnić mechanizm zliczania nieudanych prób zameldowania się do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcję.
3. Wszystkie logi opisujące pracę systemu, zameldowania i wymeldowania użytkowników oraz rejestr z systemu śledzenia wykonywanych operacji w programie należy przed usunięciem zapisać na płytę CD-R/DVD-R.

C. Rejestracja działań konserwacyjnych, awarii oraz napraw

1. Administrator Bezpieczeństwa Systemu Informatycznego prowadzi „Dziennik Systemu Informatycznego Szpitala”. Wzór i zakres informacji rejestrowanych w dzienniku określony jest w **Załączniku Nr 3**.
2. Wpisów do dziennika może dokonywać Administrator Danych Osobowych, Administrator Bezpieczeństwa Systemu Informatycznego lub osoby przez nich wyznaczone.

XI. Sieć LAN oraz dostęp do Bibliotek.


W lokalnej sieci komputerowej eksploatowanej w Szpitalu wydzielone są logicznie trzy podsieci:

- podsieć Szpitala – z dostępem do rozległej;
- podsieć Laboratorium – bez dostępu do sieci rozległej;
- podsieć akademicka CM UMK – zarządzana przez administratorów z CM UMK.

Pracownicy Szpitala mogą w sposób nieograniczony korzystać z zasobów Open Access (Otwarty Dostęp) - wolny, bezpłatny, powszechny, trwały i natychmiastowy dostęp do danych i publikacji elektronicznych o charakterze naukowym i edukacyjnym.

Każdy użytkownik sieci ma prawo czytać, kopiować, drukować, rozpowszechniać, indeksować, cytować oraz przeszukiwać zasoby otwarte, w tym pełne teksty artykułów opublikowanych w modelu Open Access, bez ograniczeń finansowych, prawnych i technicznych, przy zachowaniu praw autorskich.

Pracownicy naukowcy oraz studenci na podstawie odrębnych zasad posiadają poprzez wydzieloną podsieć dostęp do zasobów sieci CM UMK.


	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 9 z 31 PR1.3_SD1_w1

XII. Połączenie do sieci Internet.

- 1) Połączenie komputerów eksploatowanych w lokalnej sieci komputerowej Szpitala z Internetem jest dopuszczalne wyłącznie po zainstalowaniu mechanizmów ochronnych - firewall oraz kompleksowego oprogramowania antywirusowego.
- 2) Każdy pracownik ma dostęp do Internetu poprzez router brzegowy Szpitala.
- 3) Dostęp do Internetu jest monitorowany przez administratorów poprzez zbieranie logów z routera brzegowego.
- 4) Każdy pracownik ma prawo do przeglądania stron:
 - instytucji rządowych, które charakteryzują się rozszerzeniem domeny.gov.pl.;
 - stron internetowych tematycznie dotyczących wykonywanych przez niego obowiązków.
- 5) Zabrania się:
 - a. przeglądania i udostępniania treści zakazanych np. strony o charakterze pornograficznym, nazistowskim, antysemickim, rasistowskim i itp.;
 - b. udostępniania treści chronionych prawem autorskim (filmy, utwory muzyczne, itp.);
 - c. prowadzenia działalności komercyjnej;
 - d. uruchamiania gier komputerowych;
 - e. korzystania z serwerów mających charakter wyłącznie rozrywkowy;
 - f. korzystania ze stron niezgodnych z obowiązującym w Polsce prawem, zasadami współżycia społecznego, normami społeczno- obyczajowymi.
- 6) Użytkownik ponosi pełną odpowiedzialność za wszelkie szkody przez niego spowodowane w odległych lub lokalnych systemach komputerowych oraz wszelkie inne straty lub nadużycia popełnione przy użyciu udostępnionych mu zasobów Internetu i programów użytkowych.

XIII. Procedury korzystania z komputerów przenośnych


1. Poniższe zasady dotyczą komputerów przenośnych eksploatowanych przez członków Zarządu Szpitala oraz Kierownika Działu Controllingu Finansowego. Do pozostałych laptopów stosują się zasady takie, jak do zwykłych komputerów stacjonarnych.
2. Laptopy można użytkować poza terenem Szpitala wyłącznie do celów służbowych.
3. Dane na dysku laptopa wymienionego w pkt. 1 zabezpieczone są zgodnie z zasadami dotyczącymi zwykłych stacji roboczych.

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: PR 1.3	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 10 z 31 PR1.3_SD1_w1

4. Za dane przechowywane na dyskach komputera przenośnego odpowiada jego użytkownik.
5. Osoba użytkująca laptop zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania oraz odpowiada za jego stan techniczny.
6. Użytkownicy komputerów przenośnych zobowiązani są do przestrzegania zasady, aby nie pozostawiać komputera przenośnego bez nadzoru ani udostępniania go osobom trzecim.
7. Pracownik jest obowiązany do bezpiecznego przechowywania i przenoszenia laptopa.
8. Pracownik jest obowiązany zachować określone pierwotnie skonfigurowane oprogramowanie zabezpieczające dostęp do danych zgromadzonych na dysku laptopa.
9. Wszystkie uszkodzenia oraz problemy związane z działaniem dysku przenośnego należy zgłaszać do Działu Informatyki.
10. Obowiązuje zakaz korzystania z prywatnych komputerów przenośnych na terenie Szpitala.
11. Zgodę na ich eksploatację wydaje Dyrektor Szpitala na pisemną prośbę zainteresowanego. Po jej wyrażeniu Dział Informatyki przygotowuje odpowiednio prywatny komputer do pracy w sieci Szpitala.
12. Zabieranie laptopów do domu jest możliwe jedynie po otrzymaniu pisemnej zgody ADO.

XIV. Procedura korzystania z poczty wewnętrznej i Intranetu


1. Każdy pracownik ma prawo do posiadania konta poczty elektronicznej po złożeniu odpowiedniego wniosku o założenie konta poczty elektronicznej w domenę biziell.pl. Do każdego konta poczty elektronicznej przypisany jest adres e-mail, który ma postać imię.nazwisko@biziell.pl lub funkcja@biziell.pl
2. Każdy użytkownik korzystający z usługi poczty elektronicznej jest zobowiązany do korzystania z tej usługi w sposób zgodny z obowiązującym w Polsce prawem, zasadami współżycia społecznego, normami społeczno-obyczajowymi i szeroko pojętymi zasadami „netykiety”. W szczególności zakazane jest (i jest rozumiane za naruszenie postanowień niniejszego ustępu):
 - rozsyłanie spamu (w tym "niechcianej" poczty, "niechcianej" reklamy, reklamy), rozsyłanie treści sprzecznych z prawem, naruszających zasady współżycia społecznego oraz powszechnie akceptowalne normy społeczno-obyczajowe;
 - podszywanie się pod inne osoby;
 - naruszanie w jakikolwiek inny sposób dóbr osobistych osób trzecich;
 - naruszanie tajemnicy korespondencji;
 - inne zachowanie użytkownika, które zostaną uznane przez ASI lub administratora za zachowania niepożądane, w tym w szczególności zachowania polegające na istotnym obciążaniu serwerów lub łączy Szpitala.
3. Poczta elektroniczna powinna być odbierana codziennie. Zalecane jest sprawdzanie poczty najczęściej, jak jest to możliwe.

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: PR 1.3	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 11 z 31 PR1.3_SD1_w1

4. Zabrania się podejmowania prób wykorzystania obcego konta, uruchamiania aplikacji deszyfrujących hasła innych użytkowników, prowadzenia działań mających na celu podsłuchiwanie lub przechwytywanie informacji przepływającej w sieci.
5. Przynajmniej raz w miesiącu należy usunąć zbędne wiadomości i przeprowadzić kompaktowanie wszystkich folderów. Administrator systemu będzie prowadził stały monitoring zajętości profilu użytkownika. W przypadku przepełnienia skrzynki pocztowej nieodebranymi wiadomościami (pow. 100 MB) ASI blokuje konto użytkownika i informuje o tym fakcie bezpośredniego przełożonego pracownika.
6. Należy kasować (SHIFT+DEL) niezwłocznie listy elektroniczne ostrzegające przed wirusami i innym niepożądanym oprogramowaniem a także wszelką niezidentyfikowaną korespondencję.
7. W żadnym przypadku nie należy wykonywać poleceń zawartych w liście elektronicznym wskazującym sposób usunięcia wirusa lub innego niepożądanego oprogramowania, o ile nadawcą listu nie jest administrator systemu.
8. Należy używać polskich znaków diakrytycznych (tzw. ogonki np. "ą"), jedynie w oparciu o kodowanie ISO-8859-2 lub UTF-8. W innym przypadku nie używamy polskich liter.
9. Nie należy przysyłać pocztą plików większych niż 3,5 MB bez uprzedzenia adresata, nie zaleca się przysyłania tą drogą dużych plików.
10. Wszelka korespondencja e-mailowa prowadzona przez pracownika, a niezwiązana z działalnością jednostki powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej pracownika.
11. Pracownik może wykorzystywać swój firmowy adres poczty elektronicznej wyłącznie w celu prowadzenia korespondencji związanej z działalnością służbową.
12. Firmowy adres poczty elektronicznej pracowników został utworzony na serwerach pocztowych firmy świadczącej usługi hostingowe dla Szpitala.
13. Pracodawca ma możliwość wglądu w korespondencję firmową kierowaną na adres firmowy pracownika.
14. Nie wolno wysyłać żadnych dokumentów zawierających dane osobowe na swoją prywatną skrzynkę pocztową.
15. Nie wolno ustawiać przekierowania poczty poza domenę biziel.pl, za wyjątkiem szczególnych przypadków, na które zgodę wydaje ADO.
16. W przypadku naruszenia przez pracownika zasad określonych w pkt 4 - 15 ASI blokuje dostęp do kont użytkownika i o fakcie tym powiadamia bezpośredniego przełożonego pracownika oraz ABI.
17. W przypadku pracownika, z którym został rozwiązany stosunek pracy, ASI zobowiązany jest zarchiwizować dane użytkownika, a następnie zablokować konto.

XV. Procedura dostępu zdalnego do sieci Szpitala

1. Dostęp zdalny do sieci Szpitala jest możliwy tylko w uzasadnionych przypadkach i za zgodą ASI.
2. W celu uzyskania danych dostępowych należy złożyć odpowiedni wniosek (**załącznik nr 4**).

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: PR 1.3	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 12 z 31 PR1.3_SD1_w1

3. Dane dostępne są indywidualne i przypisane do jednej konkretnej osoby (lub podmiotu) i nie mogą być przekazywane osobom nieupoważnionym

4. Użytkownik, który uzyska dostęp do sieci jest zobowiązany do:

- utrzymywania danych dostępowych w tajemnicy, a w przypadku ich utraty bądź podejrzenia dostęp do nich przez osoby trzecie do zgłoszenia celem zablokowania,
- wykorzystywania dostępu jedynie do wykonywania obowiązków służbowych (powierzonych zadań) lub wykonania prac zleconych (podmioty zewnętrzne).
- stosowania ochrony antywirusowej, indywidualnych zapór ogniowych, ochrony przed przesłankami niechcianymi (spam) oraz stałej aktualizacji oprogramowania systemowego i użytkowego.

5. Zabrania się:

- skanowania i podsłuchiwanie ruchu sieciowego; nieuzgodnionego przełamывania zabezpieczeń systemów komputerowych,
- nieuprawnionego kopiowania oprogramowania i danych.

6. W przypadku stwierdzenia naruszenia w/w zasad konto dostępne zostanie zablokowane, a względem osoby, która dopuściła się naruszenia mogą zostać wyciągnięte dalsze konsekwencje.


XVI. Odpowiedzialność

1. ADO odpowiedzialny jest za:

- ❖ podejmowanie decyzji o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych;
- ❖ upoważnianie poszczególnych osób do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;
- ❖ wyznaczania ABI oraz określania zakresu jego zadań i czynności;
- ❖ wyznaczania ABI jako właściwego do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych oraz pozostałej dokumentacji z zakresu ochrony danych;
- ❖ podejmowania odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych;
- ❖ zatwierdzania dokumentacji ochrony danych osobowych.

2. ABI odpowiedzialny jest za:

- opracowanie i aktualizację dokumentacji ochrony danych osobowych;
- wdrażanie ww. dokumentacji i kontrolowanie wykonywania zawartych w niej procedur;
- prowadzenie szkoleń z nowo zatrudnionymi pracownikami Szpitala;
- organizowanie szkoleń dla pracowników Szpitala;
- kontrolowanie eksploatacji systemu SIMPLE wraz z podsystemami kadry i płace.
- nadzorowanie wdrożenia stosownych środków organizacyjnych i technicznych w celu zapewnienia bezpieczeństwa danych;

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 13 z 31 PR1.3_SD1_w1

- nadzorowanie funkcjonowania systemu zabezpieczeń;
- prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
- nadzorowanie udostępnianiem danych osobowych odbiorcom danych i innym podmiotom;
- przygotowanie wniosków zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz prowadzenie innej korespondencji z Generalnym Inspektorem Ochrony Danych Osobowych;
- podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu informatycznego;
- prowadzenie konsultacji z Działem Informatyki dotyczących wyboru technologii informatycznych wykorzystywanych do przetwarzania danych osobowych minimalizujących zagrożenia;

3. ASI odpowiedzialni są za:

- zarządzanie systemami informatycznymi, w których przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;
- przeciwdziałanie dostępowi osób niepowołanych do systemów informatycznych, w którym przetwarzane są dane osobowe;
- wykonanie nadania i odebrania uprawnień użytkownikom zgodnie z zasadami określonymi w Instrukcji;
- nadzorowanie działania mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
- podejmowanie działań w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego;
- zmienię hasła dostępu w poszczególnych stacjach roboczych, ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby ABI lub ADO;
- w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informowanie ABI i ADO o naruszeniu i współdziałanie z nim przy usuwaniu skutków naruszenia;
- sprawowanie nadzoru nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
- podejmowanie działań służących zapewnieniu niezawodności zasilania serwerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: PR 1.3	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 14 z 31 PR1.3_SD1_w1

ZAŁĄCZNIK NR 1

REJESTR UŻYTKOWNIKÓW I UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

Znajduje się pod linkiem: <http://pisz/aplikacje/SiUsers/examples/example.php>

ZAŁĄCZNIK NR 2

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH

Niniejsza instrukcja reguluje postępowanie pracowników Szpitala zatrudnionych przy przetwarzaniu danych osobowych w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych /Rozporządzenie Ministra Spraw Wewnętrznych i administracji z dnia 29 kwietnia 2004r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych/

§1


Celem niniejszej instrukcji jest określenie zadań pracowników w zakresie:

1. ochrony danych przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą oraz ochroną zasobów technicznych,
2. prawidłowego reagowania pracowników zatrudnionych przy przetwarzaniu danych w przypadku stwierdzenia naruszenia ochrony danych osobowych lub zabezpieczeń systemu informatycznego.

§2

Naruszenie systemu ochrony danych osobowych może zostać stwierdzone na podstawie oceny:

1. stanu urządzeń technicznych,
2. zawartości zbiorów danych osobowych,
3. sposobu działania programu lub jakości komunikacji w sieci teleinformatycznej,
4. metod pracy (w tym obiegu dokumentów).

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 15 z 31 PR1.3_SD1_w1

§3.

W przypadku stwierdzenia naruszenia ochrony danych osobowych należy bezzwłocznie:

1. powiadomić Administratora Bezpieczeństwa Informacji, bezpośredniego przełożonego lub Dyrektora Szpitala,
2. zablokować dostęp do systemu dla użytkowników oraz osób nieupoważnionych,
3. podjąć działania mające na celu zminimalizowanie lub całkowite wyeliminowanie powstałego zagrożenia - o ile czynności te nie spowodują przekroczenia uprawnień pracownika,
4. zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia bezpieczeństwa systemu.

§4.

1. Bezpośredni przełożony pracownika po otrzymaniu powiadomienia o naruszenia bezpieczeństwa danych osobowych jest zobowiązany niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji lub Dyrektora Szpitala, chyba, że zrobił to pracownik, który stwierdził naruszenie.
2. Na stanowisku, na którym stwierdzono naruszenie zabezpieczenia danych Administrator Bezpieczeństwa Informacji i osoba przełożona pracownika przejmują nadzór nad pracą w systemie odsuwając jednocześnie od stanowiska pracownika, który dotychczas na nim pracował, aż do czasu wydania odmiennej decyzji.


§5.

Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona podejmuje czynności wyjaśniające mające na celu ustalenie:

1. przyczyn i okoliczności naruszenia bezpieczeństwa danych osobowych,
2. osób winnych naruszenia bezpieczeństwa danych osobowych,
3. skutków naruszenia.

§6.

1. Administrator Bezpieczeństwa Informacji zobowiązany jest do powiadomienia o zaistniałej sytuacji Dyrektora Szpitala, który podejmuje decyzje o wykonaniu czynności zmierzających do przywrócenia poprawnej pracy systemu oraz o ponownym przystąpieniu do pracy w systemie.
2. Administrator Bezpieczeństwa Informacji zobowiązany jest do sporządzenia pisemnego raportu na temat zaistniałej sytuacji, zawierającego, co najmniej:
 - a. datę i miejsce wystąpienia naruszenia,
 - b. zakres ujawnionych danych,
 - c. przyczynę ujawnienia, osoby odpowiedzialne oraz stosowne dowody winy,

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 16 z 31 PR1.3_SD1_w1


- d. sposób rozwiązania problemu,
- e. przyjęte rozwiązania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

Raport ten Administrator Bezpieczeństwa Informacji przekazuje Dyrektorowi Szpitala.

§7.

Za naruszanie ochrony danych osobowych obowiązują następujące kary:

1. Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
2. Kto będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
3. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności lub pozbawienia wolności do roku.
4. Kto narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
5. Za naruszenie ochrony danych osobowych Dyrektor Szpitala może stosować kary porządkowe, niezależnie od zastosowania kar, o których mowa wyżej.

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 17 z 31 PR1.3_SD1_w1

ZAŁĄCZNIK NR 3

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego, a w szczególności:

- w przypadku awarii - opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;*
- w przypadku konserwacji systemu - opis podjętych działań, wnioski*


DZIENNIK SYSTEMU INFORMATYCZNEGO SZPITALA składa się z dwóch dokumentów prowadzonych elektronicznie:

1. Zgłoszenia serwisowe – znajduje się pod linkiem:

<http://pisz/zgloszenia/zgloszenia.php>

2. Rejestr incydentów – znajduje się pod linkiem:

<http://pisz/zgloszenia/wykonane.php?incydenty=Incydenty>

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 18 z 31 PR1.3_SD1_w1

ZAŁĄCZNIK NR 4

Wniosek o uzyskanie dostępu zdalnego do zasobów sieci informatycznej Szpitala Uniwersyteckiego nr 2 Im. Dr. Jana Biziela w Bydgoszczy

Imię i nazwisko, nazwa użytkownika	
Jednostka organizacyjna	
Cel dostępu (aplikacje, bazy itp.)	
Uzasadnienie	
Skąd realizowany ma być dostęp zdalny (sieci, adresy, komputery itp.)	
Okres obowiązywania	

Oświadczam, że znana jest mi treść Standardu Zarządzania Systemem Informatycznym Sieci Komputerowej Szpitala Uniwersyteckiego nr 2 im. Dr. Jana Biziela w Bydgoszczy oraz Polityki Bezpieczeństwa Standardu Zarządzania Systemem Informatycznym szczególnie w Zakresie Przetwarzania Danych Osobowych.

.....
Wnioskodawca/przełożony (data, podpis)


Oświadczam, że dołożę wszelkich starań o bezpieczeństwo informacji podczas pracy zdalnej w systemach informatycznych Szpitala Uniwersyteckiego nr 2 im. dr. Jana Biziela w Bydgoszczy.

.....
Użytkownik (data, podpis)

.....
Akceptacja Administratora Systemu Informatycznego (data, podpis)

Parametry dostępu zdalnego (wypełnia Administrator Systemu Informatycznego)	
Usługi/aplikacje dostępne w ramach dostępu zdalnego	
Sieci, z których możliwe jest połączenie zdalne	
Użyta metoda zabezpieczenia transmisji	
Pomocnicze parametry uwierzytelniania	
Miejsce instalacji oraz właściciel stanowiska zdalnego	

.....
Administrator Systemu Informatycznego (data, podpis)

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 19 z 31 PR1.3_SD1_w1

POLITYKA BEZPIECZEŃSTWA


Szpitala Uniwersyteckiego Nr 2 im. dr. Jana Bizuela w Bydgoszczy

Spis treści:

1	Cel i zakres Polityki	str. 20
2	Informacje wstępne	str. 20
3	Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe	str. 21
4	Wykaz zbiorów danych osobowych i programów zastosowanych do przetwarzania danych	str. 21
5	Obszar przetwarzania danych osobowych	str. 22
6	Opis struktury zbiorów	str. 23
7	Przepływ danych pomiędzy poszczególnymi systemami	str. 23
8	System zabezpieczeń danych osobowych	str. 24
9	Bezpieczeństwo Serwerów, Sieci i Stacji	Str. 26
10	Przeglądy i aktualizacje Polityki Bezpieczeństwa	str. 26
11	Postanowienia końcowe	str. 27
12	Wykaz obowiązujących polityk	str. 27
	Załączniki	str. 28

Załącznik nr 1 – Schemat blokowy rozmieszczenia budynków

Załącznik nr 2 – Opis struktury zbiorów w przetwarzanych systemach

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 20 z 31 PR1.3_SD1_w1

1. Cel i zakres Polityki

1. Celem Polityki jest określenie kierunków działań oraz wsparcia dla zapewnienia bezpieczeństwa przetwarzania zbiorów danych w Szpitalu Uniwersyteckim Nr 2 im. dr. J.Biziela w Bydgoszczy (dalej zwany Szpitalem).
2. Przez bezpieczeństwo danych rozumie się zapewnienie ich poufności, integralności i dostępności oraz zapewnienie rozliczanie działań.
3. Szpital zarządza bezpieczeństwem danych w celu zapewnienia sprawnego i zgodnego z przepisami prawa wykonywania swoich zadań oraz zadań wykonywanych na podstawie umów lub powierzonych do wykonania na podstawie porozumień.
4. Zakres przedmiotowy stosowania niniejszej Polityki obejmuje wszystkie zbiory danych przetwarzane w Szpitalu w formie elektronicznej. W zakresie podmiotowym Polityka obowiązuje wszystkich pracowników Szpitala oraz inne osoby mające dostęp do danych osobowych, w tym stażystów, osoby zatrudnione na umowę zlecenia lub umowę o dzieło itp.


2. Informacje wstępne

2.1 Podstawa prawna

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926 z późn. zm.).
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z. 2004 r. Nr 100, poz. 1024).
3. Zarządzenie Nr 46/2007 Marszałka Województwa Kujawsko-Pomorskiego z dnia 15 października 2007 r.

2.2 Terminologia

1. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
2. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: PR 1.3	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 21 z 31 PR1.3_SD1_w1

określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

3. **Zbiór danych osobowych** – posiadający strukturę zestaw danych o charakterze osobowym.
4. **Nazwa użytkownika** – jednoznacznie przypisany jednej osobie identyfikator składający się z liter i cyfr, określający użytkownika w systemie informatycznym.
5. **Hasło** - ciąg znaków, stanowiący tajemnicę użytkownika, w połączeniu z nazwą użytkownika umożliwiającą uwierzytelnienie w systemie informatycznym.
6. **Administrator Bezpieczeństwa Informacji** - należy przez to rozumieć pracownika szpitala wyznaczonego do nadzorowania przestrzegania zasad ochrony danych osobowych ustanowionego zgodnie z Zarządzeniem Dyrektora Szpitala Uniwersyteckiego Nr 2.im.dr.J.Biziela,
7. **Administrator Systemu Informatycznego** - należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu teleinformatycznego szpitala oraz stosowanie technicznych i organizacyjnych środków ochrony,

3. Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe

SZPITAL – Bydgoszcz, ul. Ujejskiego 75

1DP – Przychodnia, 1DL – Przychodnia – pomieszczenia administracji szpitala, rejestracje.
1BL – Diag_Zab, 1BP – Diag-Zab – Oddziały Szpitala,
1AL – Blok Łóżek, 1AP- Blok Łóżek – Oddziały Szpitala
1C – Pom.Dor. - Ratwonicstwo, Izby Przyjęć,
1H – Pawilon Dziecięcy – Oddziały Szpitala,
7A – Pawilon Łóżkowy, 7B – Pawilon Łóżkowy – Oddziały Szpitala.
7C – Samodzielna Sekcja Informatyki.
Schemat blokowy rozmieszczenia budynków zawiera załącznik nr 1 do niniejszej Polityki.


4. Wykaz zbiorów danych osobowych i programów zastosowanych do przetwarzania danych.

1. Dział Zarządzania Zasobami Ludzkimi

Zbiór danych: Ewidencja kadrowo pracowników szpitala, Wolontariusze, Staże częstkowe

Programy zastosowane do przetwarzania danych:

- System Wspomagający Zarządzanie Przedsiębiorstwem SIMPLE-SYSTEM V,
- PŁATNIK – system przekazu elektronicznego danych do ZUS,
- Oprogramowanie biurowe: OpenOffice i MS Office

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: PR 1.3	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 22 z 31 PR1.3_SD1_w1

2. Działu Wynagrodzeń i Umów Cywilnoprawnych

Zbiór danych: Ewidencja płacowa pracowników szpitala

Programy zastosowane do przetwarzania danych:

- System Wspomagający Zarządzanie Przedsiębiorstwem SIMPLE-SYSTEM V,
- PŁATNIK – system przekazu elektronicznego danych do ZUS,
- Oprogramowanie biurowe: OpenOffice i MS Office

3. Dział Księgowości

Zbiór danych: kartoteka kontrahentów, należności i zobowiązania, system finansowo-księgowy.

Programy zastosowane do przetwarzania danych:

- System Wspomagający Zarządzanie Przedsiębiorstwem SIMPLE-SYSTEM V,
- System bankowości elektronicznej – platforma webowa
- Oprogramowanie biurowe: OpenOffice i MS Office

4. Dział Obsługi Pacjenta

Zbiór danych: Dane świadczeniobiorców

Programy zastosowane do przetwarzania danych:

Dziedzinowe programy – **RUCH CHORYCH**

System Zarządzania Obiegiem Informacji - SZOI

Oprogramowanie biurowe: OpenOffice i MS Office

5. Dział Zamówień Publicznych i Zaopatrzenia

Zbiór danych: Zamówienia publiczne

Programy zastosowane do przetwarzania danych:

- Obieg Spraw i Dokumentów, Zamówienia
- System Wspomagający Zarządzanie Przedsiębiorstwem SIMPLE-SYSTEM V,

6. Oddziały Szpitala

Zbiór danych: Dane świadczeniobiorców


Programy zastosowane do przetwarzania danych:

- Dziedzinowe programy – **RUCH CHORYCH**
- (Izba Przyjęć, Statystyka, Kontrakt, Przychodnia, Oddział, Ruch Chorych, Fakturowanie, Labo, IMPAX, Cabinet)

Wszystkie komórki organizacyjne eksploatują program Planowanie Pracy

5. Obszar przetwarzania danych

1. Obszar przetwarzania danych obejmuje pomieszczenia Działu Zarządzania Zasobami Ludzkimi, Działu Wynagrodzeń i Umów Cywilnoprawnych, Działu Księgowości, Działu

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: PR 1.3	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 23 z 31 PR1.3_SD1_w1

Obsługi Pacjenta oraz na Oddziałach Szpitala wybrane pomieszczenia (gabinety lekarskie, pomieszczenia pielęgniarek oddziałowych oraz dyżurki pielęgniarek).

2. Pomieszczenia w bloku 7C (suterena) to pomieszczenia Administratorów Systemów. W uzasadnionych przypadkach (np. awaria) administratorzy mogą także uzyskać dostęp do systemów z dowolnego pomieszczenia, w którym jest sieć komputerowa. Uzyskiwanie takiego dostępu przez innych użytkowników jest zabronione.



6. Opis struktury zbiorów

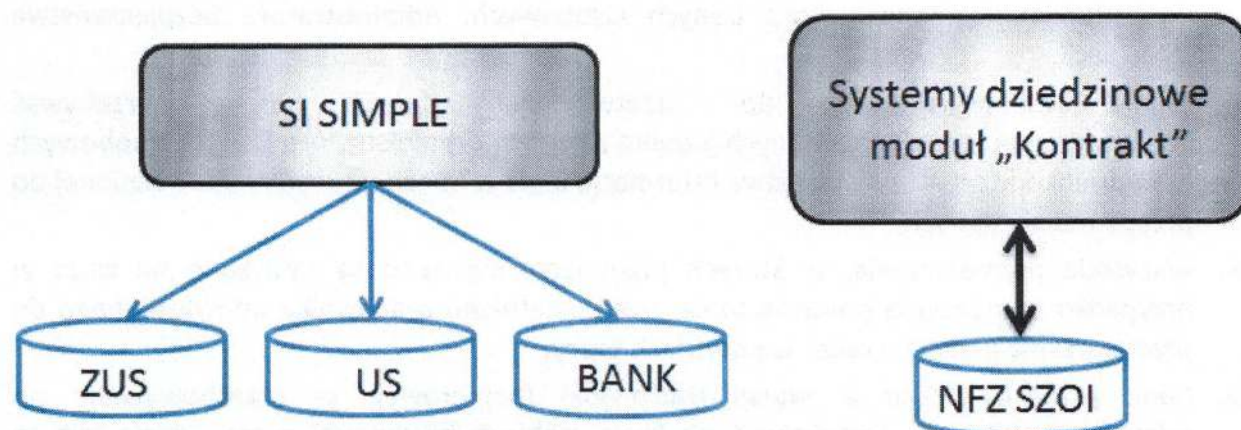
Opis struktury zbiorów zawiera załącznik nr 2 do niniejszej Polityki.

7. Przepływ danych pomiędzy poszczególnymi systemami


Przepływ danych pomiędzy systemami przedstawia Rysunek 7-1. W przypadku pozostałych zbiorów systemów i zbiorów dane są wykorzystywane wyłącznie przez aplikację powiązaną ze zbiorem – nie ma przepływu danych.

LEGENDA

-  Zbiór danych osobowych, System Informatyczny
-  Odczyt i zapis informacji wykonywany przez system informatyczny




Rysunek 7-1 Przepływ danych pomiędzy niektórymi systemami

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 24 z 31 PR1.3_SD1_w1


8. System zabezpieczeń danych

Zestawienie środków organizacyjnych i technicznych zapewniających ochronę danych osobowych w zakresie poufności, integralności i rozliczalności.

1. Każda osoba przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych, a w szczególności z przepisami karnymi.
2. Osoby zatrudnione przy przetwarzaniu danych osobowych, mające do nich dostęp, zobowiązane są do zachowania ich tajemnicy zarówno w czasie zatrudnienia, jak i po jego ustaniu.
3. Ochrona zbiorów danych polega na zabezpieczeniu informacji wprowadzonej, przetwarzanej, przesyłanej w systemie informatycznym oraz na nośnikach informacji przed nielegalnym ujawnieniem, kradzieżą oraz nieuprawnioną modyfikacją lub usunięciem.
4. W celu ochrony danych przechowywanych w systemach informatycznych należy wykorzystywać wchodzące w ich skład mechanizmy zarówno sprzętowe jak i programowe oraz inne rozwiązania zwiększające bezpieczeństwo danych.
5. Dane osobowe mogą przetwarzać wyłącznie osoby posiadające upoważnienia do przetwarzania danych osobowych. Osoby upoważnione do przetwarzania danych mają obowiązek zachować w tajemnicy dane, które przetwarzają, oraz sposoby ich zabezpieczenia.
6. W przypadku żądania udostępniania danych pracownicy Szpitala postępują zgodnie z przepisami ustawy o ochronie danych osobowych. Decyzję podejmuje pracownik po powiadomieniu Administratora Danych Osobowych, Administratora Bezpieczeństwa Informacji.
7. Osoby nieupoważnione do przetwarzania danych mogą przebywać w obszarach przetwarzania danych jedynie za zgodą Administratora Danych Osobowych lub Administratora Bezpieczeństwa Informacji, bądź w obecności osoby upoważnionej do przetwarzania danych.
8. Wszystkie pomieszczenia, w których przetwarza się dane są zamykane na klucz w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych – także w godzinach pracy.
9. Dane przechowywane w wersji tradycyjnej (papierowej) są przechowywane po zakończeniu pracy w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe – w szafach metalowych lub pancernych. Klucze od szafek należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych.
10. Urządzenia, dyski lub inne elektroniczne nośniki danych, zawierające dane przeznaczone do:

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: PR 1.3	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 25 z 31 PR1.3_SD1_w1

- a) likwidacji – pozbawia się zapisu tych danych lub uszkadza w sposób uniemożliwiający ich odczytanie,
 - b) naprawy – pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.
11. Dane w wersji papierowej, a także wydruki i kopie, należy niszczyć w niszczarkach. Zabronione jest usuwanie danych przez wyrzucenie ich do kosza na odpadki.
 12. Budynki, w których zlokalizowane są zbiory danych, są nadzorowane przez pracowników ochrony przez całą dobę.
 13. Dla danych osobowych przetwarzanych w systemach informatycznych stosuje się następujące zasady:
 - a) kontrola dostępu do zbiorów danych osobowych,
 - b) indywidualne identyfikatory użytkowników (pracowników przetwarzających dane osobowe),
 - c) uwierzytelnianie użytkowników (potwierdzanie ich tożsamości).
 14. W celu zabezpieczenia danych osobowych przed ich utratą lub uszkodzeniem:
 - a) dla wszystkich systemów wdrożono polityki kopii zapasowych,
 - b) wszystkie systemy informatyczne wyposażono w awaryjne zasilanie,
 - c) wdrożono oprogramowanie antywirusowe,
 - d) dostęp do systemów z sieci publicznej jest kontrolowany za pomocą zapory sieciowej oraz filtrów antyspamowych i oprogramowania antywirusowego,
 - e) przy przesyłaniu danych osobowych przez sieć publiczną użytkownicy są zobowiązani stosować oprogramowanie szyfrujące PGP.
 15. Użytkowników systemów przetwarzających dane osobowe obowiązuje następująca polityka haseł:
 - a) minimalna długość hasła wynosi 8 (osiem) znaków,
 - b) zmiana hasła nie rzadziej niż co 30 dni,
 - c) hasło zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
 16. Jeżeli system informatyczny środkami technicznymi nie wymusza zasad ujętych w pkt. 15 użytkownik zobowiązany jest do przestrzegania powyższych zasad, a tym samym do okresowej zmiany hasła i dobrania odpowiedniej jego długości.
 17. Użytkownik, który utracił hasło, zobowiązany jest zgłosić ten fakt bezzwłocznie do ABI lub ASI.
 18. Użytkownik nie ma prawa samodzielnie podłączać do sieci teleinformatycznej urządzeń aktywnych. Zgodę na podłączenie wydaje Administrator Systemu Informatycznego.
 19. Niedopuszczalne jest samodzielne włączania do sieci teleinformatycznej Szpitala komputerów przenośnych, może odbyć się za pisemną zgodą Dyrektora Szpitala.

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 26 z 31 PR1.3_SD1_w1


20. Zabronione jest nawiązywanie połączeń głosowych i video za pośrednictwem komunikatorów internetowych, oraz używanie oprogramowania P2P.
21. Niedopuszczalna jest samodzielna przez użytkowników rozbudowa sieci lokalnej Szpitala o segmenty wykorzystujące technologię dostępu radiowego (WiFi).

9. Bezpieczeństwo Serwerów, Sieci i Stacji

Zalecenia i wymogi dotyczące eksploatacji serwerów, sieci, stacji roboczych zostały opisane w dokumencie BEZPIECZEŃSTWO SIECI, SERWERÓW I STACJI, opublikowanym w PISZ pod linkiem: <http://pish/index.php?it=56>

10. Przeglądy i aktualizacje Polityki

1. Polityka bezpieczeństwa podlega przeglądowi pod kątem aktualności i stosowności nie rzadziej niż raz do roku. Przeglądu dokonuje Administrator Systemu Informatycznego.
2. Polityka bezpieczeństwa podlega aktualizacji każdorazowo w przypadku:
 - a) likwidacji, utworzenia lub zmiany zawartości informacyjnej zbioru,
 - b) zmiany lokalizacji zbioru,
 - c) zmiany przepisów prawa dotyczącego ochrony danych osobowych, wymagającej aktualizacji Polityki,
 - d) innych znaczących zmian dotyczących danych osobowych w funkcjonowaniu Urzędu.
3. Aktualizacji Polityki dokonuje Administrator Bezpieczeństwa SI. Zatwierdzenia zaktualizowanej Polityki dokonuje Dyrektor Szpitala.

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 27 z 31 PR1.3_SD1_w1

11. Postanowienia końcowe

1. ASI lub upoważniony pracownik Działu Informatyki w porozumieniu z Dział Zarządzania Zasobami Ludzkimi przeprowadza szkolenia pracowników i nowozatrudnionych pracowników w zakresie przepisów prawa oraz uregulowań wewnętrznych (Polityki Bezpieczeństwa danych osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych) w ciągu do 1-go miesiąca od dnia zatrudnienia.
2. Szkolenie z bezpieczeństwa informacji w szczególności obejmuje:
 - a. zagadnienia związane z przestrzeganiem zasad obowiązujących w Szpitalu;
 - b. konsekwencje ich nieprzestrzegania.
3. Po zakończeniu szkolenia pracownik podpisuje stosowne oświadczenie.

12. Wykaz obowiązujących polityk

Lp	Nazwa	Numer
1	Polityka klasyfikacji informacji	PR1.3_PI6_w1
2	Bezpieczeństwo sieci, serwerów i stacji	PR1.3_PI7_w1
3	Polityka zabezpieczenia kryptograficznego	PR1.3_PI8_w1
4	Polityka nadawania uprawnień w systemie	PR1.3_PI9_w1
5	Polityka tworzenia kopii bezpieczeństwa	PR1.3_PI10_w1
6	Procedura zarządzania incydentami	PR1.3_PI11_w1
7	Reagowanie na incydenty bezpieczeństwa	PR1.3_PI12_w1
8	ZBI w relacjach z dostawcami	PR1.3_PI13_w1



Standard Zarządzania Systemem Informatycznym
Instrukcja Zarządzania Systemem Informatycznym
Polityka Bezpieczeństwa

ISO 9001
ISO 14001
ISO 27001
PN-N 18001

Proces:

Numer procesu: PR 1.3

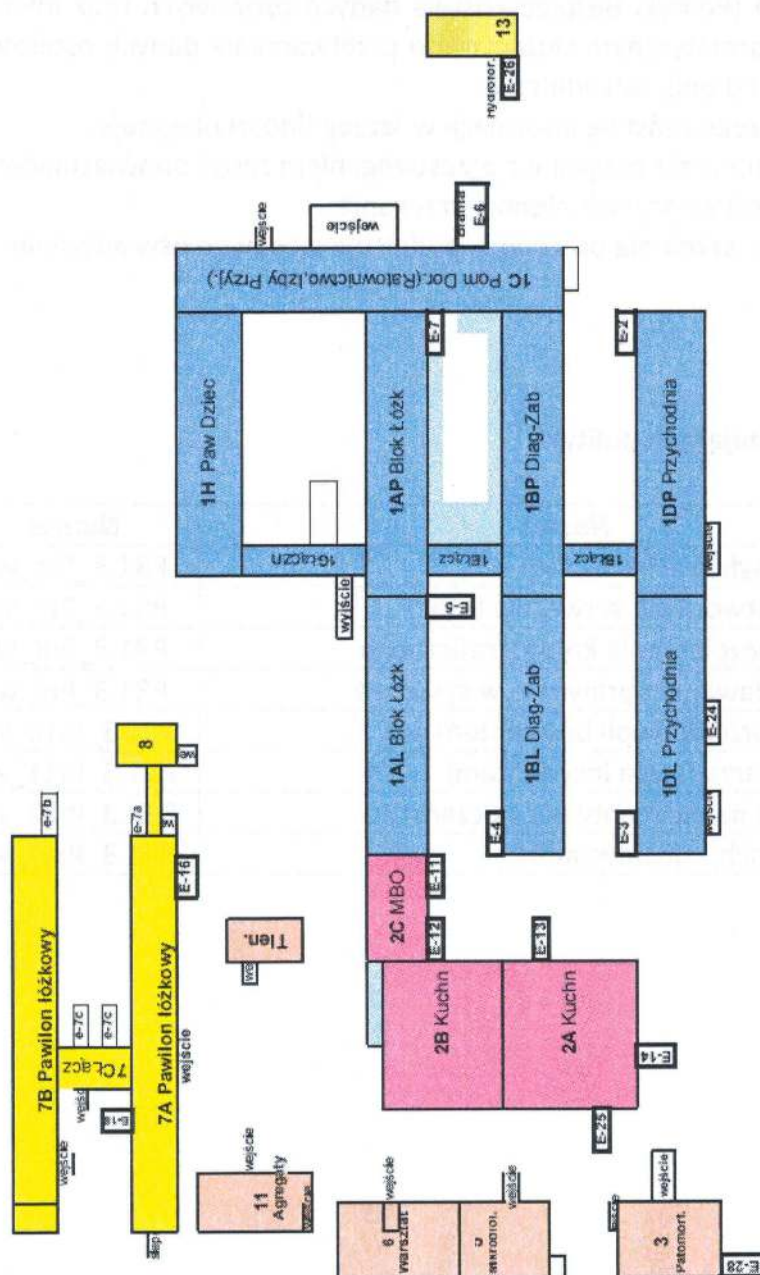
Zarządzanie Bezpieczeństwem Informacji


Strona 28 z 31

PR1.3_SD1_w1

Załącznik Nr 1

SCHEMAT BLOKOWY ROZMIESZCZENIA BUDYNKÓW
SZPITALA WOJEWÓDZKIEGO IM. J. BIZIELA W BYDGOSZCZY



	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 29 z 31 PR1.3_SD1_w1

Załącznik Nr 2

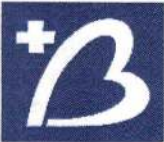
OPIS STRUKTURY ZBIORÓW W PRZETWARZANYCH SYSTEMACH

Dziedziczne Programy – RUCH CHORYCH

pesel,
plec_id,
data_urodzenia, miejsce_urodzenia,
czas_zgonu,
nazwisko, imie, imie2,
imie_ojca, imie_matki,
stan_cywilny,
imie_wspolmalzonka,
telefon,
ulica, nr_domu, nr_lokalu, miejscowosc, kod_pocztowy,
gmina, wojewodztwo, kraj, obywatelstwo,
ubezpieczenie,
adres_email,
zawod_pacjenta,
grupa_krwi, czynnik_rh,
bezdromny,
rok_nauki, uczen,
opiekun_id,
ubezpieczenie_numer,
poczta,
miejscowosc, kod_pocztowy, ulica, nr_domu, nr_lokalu, poczta, nip.

Zintegrowany System Zarządzania Przedsiębiorstwem – SIMPLE-SYSTEM V

pesel, płeć
data urodzenia, miejsce urodzenia,
nazwisko, imię, imie2,
imię ojca, imię matki, nazwisko rodowe matki,
stan cywilny,
imię współmałżonka,
telefon, poczta elektroniczna
ulica, nr domu, nr lokalu, miejscowość, kod pocztowy,
gmina, województwo, kraj,
obywatelstwo,
seria i nr dowodu osobistego,

	Standard Zarządzania Systemem Informatycznym Instrukcja Zarządzania Systemem Informatycznym Polityka Bezpieczeństwa	ISO 9001 ISO 14001 ISO 27001 PN-N 18001
Proces: Numer procesu: <i>PR 1.3</i>	<i>Zarządzanie Bezpieczeństwem Informacji</i>	Strona 30 z 31 PR1.3_SD1_w1

wykształcenie,
badania lekarskie,
specjalizacja.

System Zarządzania Obiegiem Informacji - SZOI

Dane przekazywane do systemu są w formacie xml i zawierają struktury danych osobowych jak w **RUCH CHORYCH**.

Podstawowy Program Świadczeniodawcy – KS-PPS

Dane przekazywane do systemu są w formacie xml i zawierają struktury danych osobowych jak w **RUCH CHORYCH**.