Spis treści:

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

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

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.

Ilekroć w niniejszym dokumencie jest mowa o:

a) **Szpitalu** - należy przez to rozumieć Szpital Uniwersytecki Nr 2 im. dr. J.Biziela w Bydgoszczy,

b) **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,

c) **Administratorze Systemu Informatycznego -** należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu teleinformatycznego szpitala oraz stosowanie technicznych i organizacyjnych środków ochrony,

d) **użytkowniku 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,

e) **sieci lokalnej** - należy przez to rozumieć połączenie systemów informatycznych Szpitala wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,

f) **sieci rozległej** - należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, póz. 852, z późn. zm.)

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

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
   - Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z późn. zm.),
   - Polityką bezpieczeństwa przetwarzania danych osobowych systemu informatycznego, niniejszym dokumentem.

2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi **Załącznik Nr 2.**
3. Administrator Bezpieczeństwa Systemu Teleinformacznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego wniosku pracownika, którego wzór stanowi **Załącznik** Nr **I** do niniejszego opracowania.
4. Jedynie prawidłowo wypełniony wniosek o nadanie uprawnień w systemie oraz zmianę tych uprawnień jest podstawą rejestracji uprawnień w systemie.
5. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.
6. Hasło ustanowione podczas przyznawania uprawnień przez Administrator Bezpieczeństwa Systemu Informatycznego należy zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym. Ustanowione hasło początkowe, administrator przekazuje użytkownikowi ustnie.
7. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
8. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
9. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
10. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.
11. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.
12. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.
13. Odebranie uprawnień pracownikowi następuje na pisemny wniosek kierownika, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień.
14. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administrator Bezpieczeństwa Systemu Informatycznego o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
15. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.
16. Administrator Bezpieczeństwa Systemu Informatycznego zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym.
17. Dostęp anonimowy do Internetu musi zostać poprzedzone zgodą Dyrektora Szpitala lub Kierownika DI.
18. Rejestr znajduje się w PISZ/ Dział Informatyki/Techniczny
19. Rejestr powinien odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników.

20. Uprawniony personel DI zobowiązany jest do wykonywania regularnych przeglądów istniejących uprawnień dostępu użytkowników do systemów informatycznych pod kątem weryfikowania poniższych obszarów:
    - przegląd aktywności użytkowników w systemach
    - przegląd pod kątem ważności kont użytkowników
    - przegląd pod kątem posiadania wymaganych uprawnień przez pracowników posiadających konta w systemach.

III. Zasady posługiwania się hasłami.

1. Identyfikator w systemie zbudowany jest zgodnie z zasadą pełne nazwisko pierwsza litera imienia nnnnnnnnm,
   w przypadku wystąpienia dwóch identycznych identyfikatorów na końcu dodany będzie parametr numeryczny.
2. Bezpośredni dostęp do danych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
3. Hasło użytkownika powinno być zmieniane, co najmniej raz w miesiącu, w przypadku otrzymania pierwszego hasła do systemu użytkownik jest zobowiązany natychmiast je zmienić.
4. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
5. Konta systemowe nie mogą być współdzielone przez więcej niż jednego użytkownika jak również nie mogą swoją przynależnością określać terminali komputerowych, działów w firmie lub konkretnych stanowisk.
6. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł, których nie wolno udostępniać innym osobom.
7. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
8. Pracownik nie ma prawa do udostępniania haseł danej grupy osobom spoza tej grupy, dla której zostały one utworzone.
9. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
10. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
11. Przy wyborze hasła obowiązują następujące zasady:
    a/ minimalna długość hasła - 8 znaków,
    b/ **zakazuje się stosować:**
    - haseł, które użytkownik stosował uprzednio w okresie minionego roku,
    - swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),
    - swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie,
    - imion (w szczególności imion osób z najbliższej rodziny),
    - ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, itp.
    - wyrazów słownikowych,
    - przewidywalnych sekwencji znaków z klawiatury np.: QWERTY", "12345678",itp.

    c/ **należy stosować:**
    - hasła zawierające kombinacje liter i cyfr,
    - hasła zawierające znaki specjalne:
    - ✓ znaki interpunkcyjne, nawiasy, symbole @, #, &, itp. o ile system informatyczny na to pozwala,

- hasła, które można zapamiętać bez zapisywania,
- hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim.

10. Zmiany hasła nie wolno zlecać innym osobom.
11. W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia – może wystąpić na stanowiskach roboczych w Dziale Informatyki.
12. Hasło użytkownika o prawach administratora powinno znajdować się w zalakowanej kopercie w zamykanej na klucz szafie metalowej, do której dostęp ma Administrator Systemu Informatycznego.
13. Dla osób spoza szpitala w celach serwisowych zakładanie kont odbywa się zgodnie z pkt. 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 utarty 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

- Podróże samochodem służbowym

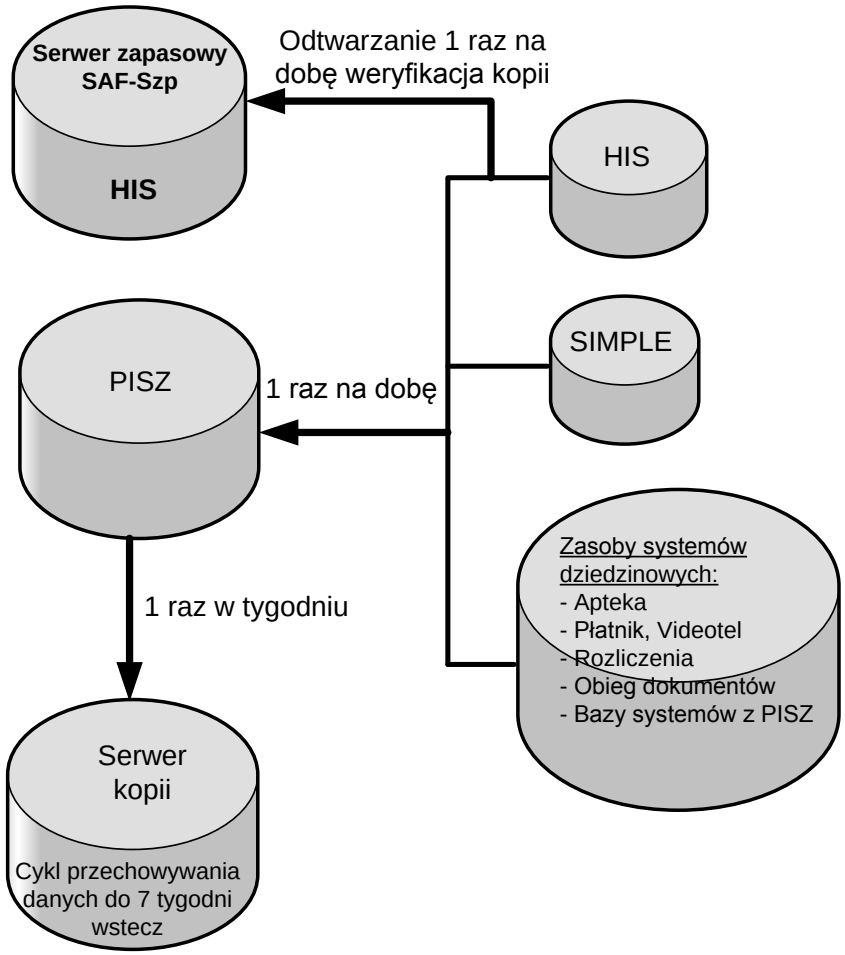
1. Pamiętaj, aby w trakcie podróży samochodem służbowym, nigdy nie pozostawiać w samochodzie żadnych dokumentów ani urządzeń teleinformatycznych Szpitala,
2. Pamiętaj, aby nie trzymać komputera w osobowej części samochodu – zawsze zamykaj komputer w bagażniku samochodu.

V. Procedury tworzenia kopii bezpieczeństwa.

1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Systemu Informatycznego, a w przypadku jego nieobecności wyznaczony pracownik z Działu Informatyki.

2. Tworzenie kopii z każdego dnia tygodnia dla systemu części białej oraz szarej (administracyjnej) odbywa się automatycznie. Wszystkie backup'y z systemów dziedzinowych

oraz zasoby domenowe archiwizowane są na serwerze „PISZ”. Następnie w każdy poniedziałek w celu weryfikacji poprawności wytworzonych kopii są kopiowane na NAS. W NAS utrzymywane są kopie przez 7 tygodni. Poniżej przedstawiono schemat wytwarzania i przechowywania kopii bezpieczeństwa.



Ścieżka dostępu do kopii na serwerze „PISZ”:

//mnt/hdd2/samba/kopie/ ..

3. Na serwerze kopii zasoby są przechowywane w cyklach 7-mio tygodniowych. Serwer znajduje się pod adresem 192.168.2.230.

4. W celu weryfikacji poprawności wykonanej kopii bezpieczeństwa systemu HIS raz na dobę wykonywane jest jej odtwarzanie na serwerze zapasowym, który wykorzystywany jest do obsługi systemu SAF-Szp.

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

A. Elektroniczne nośniki informacji.

1. Dane wg polityki klasyfikacji informacji w postaci elektronicznej – zapisane na dyskietkach, dyskach magnetooptycznych, pamięć przenośna USB czy dyskach twardych nie są wynoszone poza siedzibę Szpitala.
2. Wymienne elektroniczne nośniki informacji są przechowywane w pomieszczeniach służbowych.
3. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub kasetkach.
4. 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.
5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych.
6. 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.
7. 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.
8. Nie pozostawiaj bez opieki służbowego telefonu komórkowego
9. 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.

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.
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 jakiejkolwiek 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 4 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 Administrator Bezpieczeństwa Systemu Informatycznego.

B. Przegląd programów i narzędzi programowych.

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 5.**
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 naukowi oraz studenci na podstawie odrębnych zasad posiadają poprzez wydzieloną podsieć dostęp do zasobów sieci CM UMK.

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 programem szyfrującym dane TrueCrypt.
4. Hasło dostępu do danych na dysku przenośnym jest utworzone i znane tylko użytkownikowi dysku.
5. Długość hasła wynosi co najmniej 8 znaków (litery, cyfry lub znaki specjalne). Hasło zostaje zapisane i umieszczone w zamkniętej kopercie przechowywanej w sejfie w pomieszczeniu Kierownika Działu Informatyki.
6. Hasło do dysku przenośnego musi być zmieniane przynajmniej raz na kwartał.
7. Za czynności wymienione w punkcie 5 i 6 odpowiada użytkownik laptopa.
8. Osoba użytkująca laptop zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania oraz odpowiada za jego stan techniczny.
9. Użytkownicy komputerów przenośnych zobowiązani są do przestrzegania zasady, aby nie pozostawiać komputera przenośnego bez nadzoru ani udostępniania go osobom trzecim.
10. Pracownik jest obowiązany do bezpiecznego przechowywania i przenoszenia laptopa.
11. Pracownik jest obowiązany zachować określone pierwotnie skonfigurowane oprogramowanie zabezpieczające dostęp do danych zgromadzonych na dysku laptopa.
12. Wszystkie uszkodzenia oraz problemy związane z działaniem dysku przenośnego należy zgłaszać do Działu Informatyki.
13. Obowiązuje zakaz korzystania z prywatnych komputerów przenośnych na terenie Szpitala.
14. 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.
15. 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 domenie biziel.pl. Do każdego konta poczty elektronicznej przypisany jest adres e-mail, który ma postać imię.nazwisko@biziel.pl lub funkcja@biziel.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.
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 przesyłać pocztą plików większych niż 3,5 MB bez uprzedzenia adresata, nie zaleca się przesyłania 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. 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;
   - 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.

ZAŁĄCZNIK NR 1
DO INSTRUKCJI ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM

WNIOSEK O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

☐ **Nowy użytkownik**	☐ **Modyfikacja uprawnień**	☐ **Odebranie uprawnień w systemie informatycznym**

Imię i nazwisko użytkownika:	**Zespół/ Wydział**

Opis zakresu uprawnień użytkownika w systemie informatycznym i uzasadnienie:

- ☐ Usługi Intranetowe
- ☐ System Diagnostyki Radiologicznej
- ☐ Podsystem Ruch Chorych Moduł Przychodnia
- ☐ Podsystem Ruch Chorych Moduł Izba Przyjęć
- ☐ Podsystem Ruch Chorych Moduł Statystyka
- ☐ Podsystem Ruch Chorych Moduł Oddział
- ☐ Podsystem Ruch Chorych Moduł Bank Krwi
- ☐ Podsystem Ruch Chorych Moduł Laboratorium
- ☐ Podsystem Ruch Chorych Moduł Apteczka Oddziałowa
- ☐ Podsystem Ruch Chorych Moduł Mikrobiologia
- ☐ Dokumentacja Medyczna „Cabinet" - odczyt
- ☐ Dokumentacja Medyczna „Cabinet" - zapis
- ☐ System Analiz Finansowych – „SAF"
- ☐ Podsystem Administracyjno-Zarządczy Moduł Kadrowo-Płacowy
- ☐ Podsystem Administracyjno-Zarządczy Moduł F-K
- ☐ Podsystem Administracyjno-Zarządczy Moduł Obrót Towarowy
- ☐ Podsystem Administracyjno-Zarządczy Moduł Apteka - Centralna
- ☐ Podsystem Administracyjno-Zarządczy Moduł Majątek Trwały
- ☐ Podsystem Administracyjno-Zarządczy Moduł Fakturowanie Wewnętrzne
- ☐ Katalog pacjentów ubezpieczonych w „SZOI"
- ☐ Elektroniczny Obieg Dokumentów
- ☐ Inny, dopisz:

Data wystawienia:	Podpis bezpośredniego przełożonego użytkownika systemu:
	Podpis Administratora Systemu Informatycznego

ZAŁĄCZNIK NR 2
DO INSTRUKCJI ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM

Bydgoszcz, dnia.....

(nazwisko i imię)

(stanowisko)

OŚWIADCZENIE

Oświadczam, iż w związku z wykonywanymi obowiązkami służbowymi, przetwarzam lub mam dostęp do zbiorów, dokumentów, zestawień, kartotek lub systemów informatycznych zawierających dane osobowe i w związku z tym zapoznałem(am) się z:

1. *Ustawą z dnia 29.08.1997 r. o ochronie danych osobowych (Dz. U. Nr 133, póz. 883),*
2. *Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004r. 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. Nr 100, póz. 1024).*
3. *Dokumentem „Standard Zarządzania Systemem Informatycznym Szpitala Uniwersyteckiego Nr 2 im. dr. Jana Biziela w Bydgoszczy".*

Zobowiązuję się do bezwzględnego przestrzegania zapisów zawartych we wszystkich powyższych dokumentach.

(podpis pracownika)

ZAŁĄCZNIK NR 3
DO STANDARDU ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM

REJESTR UŻYTKOWNIKÓW I UPRAWNIEŃ
W SYSTEMIE INFORMATYCZNYM

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

ZAŁĄCZNIK NR 4
DO STANDARDU ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM

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).

§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,
   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 pozbawiania 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.

ZAŁĄCZNIK NR 5
DO STANDARDU ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM

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

Lp.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania / wnioski	Podpis