Instrukcja ZSZ POLITYKA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM		
SPZOZ PARCZEW	**Zestaw standardów akredytacyjnych 2009** **PN-EN ISO 9001** **PN-EN ISO 14001** **PN-EN ISO 45001**	**Q I-ZI 1.2 -01**
	Wydanie nr 01 **Obowiązuje od dnia 01.01.2014 r.**	**Wydanie nr 03** **obowiązuje od dnia …02.02.2021 r.….**
	(tylko na str 1) **Oryginał *** ☐ **Egzemplarz użytkowy *** ☐	(tylko na str 1) **Kopia nr**** ☐ **Wersja elektroniczna** X

* zaznaczyć x właściwie
** wpisać nr z tabeli rozdzielnika

POLITYKA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

ROZDZIAŁ I

POSTANOWIENIA OGÓLNE

§ 1

Polityka określa zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zgodnie ze strategią określoną w „Polityce Bezpieczeństwa Danych Osobowych" w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Parczewie

Dokument stanowi specyfikację podstawowych środków technicznych ochrony danych oraz elementów zarządzania systemem informatycznym. W przypadku wystąpienia potrzeb wprowadzenia nowych lub modyfikacji istniejących uregulowań proceduralnych danego obszaru, wnioski o ich opracowanie powinni składać kierownicy komórek, w których procedury są używane do Administratora Danych Osobowych bądź Inspektora Ochrony Danych. Zasady zawarte w niniejszym dokumencie oraz określone w odrębnych dokumentach powinny być udostępniane pracownikom na poszczególnych stanowiskach tylko w niezbędnym zakresie. Obowiązki wynikające z dokumentów dotyczących zarządzania systemem informatycznym oraz zasady ochrony danych osobowych należy określać w indywidualnych zakresach czynności pracowników - odpowiednio do zadań wykonywanych na zajmowanym stanowisku.

§ 2

Polityka określa, w szczególności:

1) sposób rejestrowania i wyrejestrowywania użytkowników oraz wskazuje osobę odpowiedzialną za te czynności,
2) sposób przydziału haseł dla użytkowników i częstotliwości ich zmiany oraz wskazuje osobę odpowiedzialną za te czynności,
3) procedury rozpoczęcia i zakończenia pracy,
4) metodę i częstotliwość tworzenia kopii awaryjnych,
5) metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania,
6) sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków,
7) zasady użytkowania i zarządzania oprogramowaniem
8) postępowanie w przypadku naruszenia zabezpieczenia systemu ochrony danych osobowych

§ 3

Następujące określenia w Polityce oznaczają:

- **dane osobowe** – to każda informacja dotycząca osoby fizycznej, pozwalająca na określenie tożsamości tej osoby;
- **przetwarzanie danych** - to wszelkie operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
- **Administrator Danych Osobowych (ADO) –** Dyrektor SPZOZ w Parczewie;
- **Inspektor Ochrony Danych (IOD)** - osoba odpowiedzialna za nadzorowanie przestrzegania zasad ochrony danych osobowych przetwarzanych w systemach informatycznych;
- **Administrator Systemów Informatycznych (ASI) -** osoba powołana przez dyrektora SPZOZ, której główne zadania mają na celu zabezpieczenie prawidłowego i bezpiecznego funkcjonowania systemu informatycznego
- **osoba upoważniona lub użytkownik** – osoba posiadająca upoważnienie wydane przez (ADO) i dopuszczona w zakresie w nim wskazanym, jako użytkownik do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych;
- **osoba trzecia** – to każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych lub zbiorów tych danych
- **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i urządzeń programowych zastosowanych w celu przetwarzania danych;

- **zabezpieczenie systemu informatycznego** – wdrożenie stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także utratą ich.

§ 4

Polityka ma na celu określenie procedur i właściwych warunków zarządzania systemem informatycznym dla ochrony zgromadzonych w nim danych, jak również jednolitych i bezpiecznych zasad korzystania z danych osobowych przetwarzanych w systemie informatycznym SPZOZ w Parczewie.

§ 5

Realizacja zamierzeń określonych w § 4 gwarantowana jest poprzez następujące czynności:

1) przeszkolenie użytkowników w zakresie ochrony danych osobowych oraz zapoznanie z przepisami dotyczącymi ochrony danych osobowych,
2) korzystanie z oprogramowania systemowego i użytkowego spełniającego wysokie standardy,
3) wdrażanie w systemie informatycznych zabezpieczeń gwarantujących nienaruszalną pracę systemu, w tym najnowszych wersji oprogramowania antywirusowego,
4) przypisanie użytkownikom określonych procedur pozwalających na ich identyfikację /loginy i hasła/,
5) ocena ewentualnych zagrożeń bezpieczeństwa systemu informatycznego i ryzyk związanych z jego obsługą,
6) wdrożenie zabezpieczeń o charakterze fizycznym budynków i pomieszczeń, stosownie do zagrożeń i ryzyka wynikającego z oceny, o której mowa w pkt 5,
7) stałe monitorowanie wdrożonych zabezpieczeń w celu identyfikacji podatnych na zagrożenia obszarów i słabości zabezpieczeń.

ROZDZIAŁ II
BUDYNKI, POMIESZCZENIA LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCE OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE Z UŻYCIEM STACJONARNEGO SPRZĘTU KOMPUTEROWEGO.

§ 6

1. W pomieszczeniach, w których znajduje się stacjonarny sprzęt komputerowy służący do przechowywania zbiorów danych osobowych (serwery) nie mogą być przechowywane kopie awaryjne.
2. Wejście do pomieszczeń, o których mowa w ust.1 osób nieuprawnionych jest zabronione.
3. Pomieszczenia, o których mowa w ust.1, są zabezpieczone w sposób uniemożliwiający dostęp do nich osób nieuprawnionych.
4. Niezbędne wejścia do pomieszczeń, o których mowa w ust.1, osób nieuprawnionych np. w razie wystąpienia awarii, odnotowywane jest każdorazowo w Dzienniku wizyt w serwerowni (zał. nr 4).
5. Pomieszczenia, o których mowa w ust.1, są objęte systemem monitoringu utrzymywanych warunków klimatycznych oraz zaniku zasilania.
6. Wszelkie nieprawidłowości wykryte przez system opisany w pkt 4 zgłaszane są na telefon ASI i rejestrowane w dzienniku systemu (zał. nr 1).

ROZDZIAŁ III
SPOSÓB PRZYDZIAŁU LOGINÓW I HASEŁ DLA UŻYTKOWNIKÓW I CZĘSTOTLIWOŚCI ICH ZMIANY

§ 7

Mając na uwadze, iż system informatyczny przetwarzający dane osobowe powinien być wyposażony w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu do tych danych – dla każdej osoby upoważnionej ustalany jest odrębny login i hasło. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu loginu i właściwego hasła. Hasła dostępu i loginy przyznawane są indywidualnie dla każdego z użytkowników i znane są tylko właścicielowi. Każde konto użytkownika dodatkowo w systemie ma unikalny identyfikator.

§ 8

Login użytkownika:
1) login jest niepowtarzalny;
2) po wyrejestrowaniu użytkownika z systemu informatycznego login nie jest przydzielany innej osobie;
3) login jest wpisany do rejestru osób zatrudnionych przy przetwarzaniu danych osobowych wraz z imieniem i nazwiskiem użytkownika oraz jest rejestrowany w systemie informatycznym;
4) login służy użytkownikowi do uwierzytelnienia konta i dostępu do systemu;
5) zmiana loginu jest dozwolona w przypadku zmiany nazwiska użytkownika, zachowując w dalszym ciągu ten sam identyfikator konta w systemie.

§ 9

Hasło użytkownika:
1) jest przydzielane przez ASI lub osobę wyznaczoną przez ASI, jako jednorazowe indywidualnie dla każdego z użytkowników i znane tylko użytkownikowi, który się nim posługuje;
2) zostaje zmienione przy pierwszym zastosowaniu (zalogowaniu użytkownika);
3) nie jest zapisywane w systemie w postaci jawnej;
4) jest zmieniane co najmniej raz na 30 dni;
5) jest utrzymywane w tajemnicy, również po upływie jego ważności;
6) w przypadku zapomnienia hasła, użytkownik powinien zgłosić się do ASI wyłącznie osobiście, w celu przydzielenia nowego hasła jednorazowego.

§ 10

1. Osobą odpowiedzialną w SPZOZ za sposób przydziału haseł dla użytkowników i częstotliwości ich zmiany jest ASI,
2. Hasło ASI przechowywane jest w zapieczętowanej kopercie, w miejscu wyznaczonym przez ADO.

§ 11

Przydziału i zmiany haseł dokonuje się kierując zasadami:
1) wymogiem niezbędnym jest przydział haseł alfanumerycznych skonstruowanych co najmniej
z 8 (ośmiu) znaków;
2) hasła są zmieniane przez każdego z użytkowników co najmniej raz na 30 dni. System informatyczny powinien „wymuszać" zmianę hasła, informując o upływie jego ważności;
3) hasła nie mogą składać się z prostych kombinacji znaków mogących prowadzić do odszyfrowania ich przez osoby nieuprawnione;
4) niezależnie od wymogu zmieniania haseł każdego z użytkowników co najmniej raz na 30 dni, hasło winno być zmienione przez użytkownika niezwłocznie w przypadku powzięcia podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby nieuprawnione.

§ 12

1. Użytkownik odpowiedzialny jest za wszystkie czynności wykonywane przy użyciu własnego loginu oraz hasła, którym się posługuje lub posługiwał,
2. Użytkownik jest obowiązany utrzymywać hasła, którymi posługuje się lub posługiwał, w tajemnicy, co obejmuje, w szczególności dołożenie przez niego szczególnych starań w celu uniemożliwienia zapoznania się przez osoby nieuprawnione z hasłem, nawet po ustaniu jego ważności,
3. W przypadku powzięcia przez użytkownika podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby nieuprawnione, obowiązany jest on niezwłocznie zmienić hasło i powiadomić o zdarzeniu IOD,
4. Naruszenie przez użytkownika postanowień w ust.2 lub 3 może stanowić podstawę do pociągnięcia użytkownika dla odpowiedzialności dyscyplinarnej odszkodowawczej lub karnej w trybie i na zasadach przewidzianych przepisami prawa,

ROZDZIAŁ IV
SPOSÓB REJESTROWANIA I WYREJESTROWYWANIA UŻYTKOWNIKÓW, OSOBA ODPOWIEDZIALNA ZA TE CZYNNOŚCI

§ 13

1. Rejestrowanie i wyrejestrowywanie użytkowników dokonuje ASI lub osoba wyznaczona przez ASI,
2. Kierownik Działu Kadr i Płac prowadzi rejestr użytkowników zatrudnionych w SPZOZ mających dostęp do przetwarzania i wglądu do danych osobowych oraz zbiór upoważnień, o których mowa w § 14 pkt 2 udzielanych pracownikom SPZOZ,
3. Jakiekolwiek zmiany w prowadzonej ewidencji podlegają natychmiastowemu odnotowaniu w rejestrze.

§ 14

Dana osoba jest rejestrowana w systemie informatycznym jako użytkownik po spełnieniu następujących warunków:

1) uzyskaniu przez ASI informacji koniecznych do zdefiniowania dla danej osoby jej profilu jako użytkownika oraz jej uprawnień. Informacji takich udziela bezpośredni przełożony merytorycznie odpowiedzialny co do charakteru pracy danej osoby, mającej być użytkownikiem,
2) uzyskaniu przez tą osobę upoważnienia wydanego przez ADO dopuszczającego daną osobę
w zakresie w nim wskazanym jako użytkownika, do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych. Upoważnienie wystawiane jest przez ADO, w 2 egz. (akta osobowe oraz zbiór upoważnień).

§ 15

Osoba upoważniona do dostępu i przetwarzania danych osobowych podpisuje oświadczenie o obowiązku zachowania danych osobowych w tajemnicy. Obowiązek ten trwa również po ustaniu zatrudnienia.

§ 16

Upoważnienie, o którym mowa w § 14 oraz oświadczenie, o którym mowa w § 15 Kierownik Działu Kadr i Płac dołącza do akt osobowych pracownika.

§ 17

1. Z chwilą zarejestrowania w systemie informatycznym, zgodnie z postanowieniami § 14, dana osoba jest informowana przez ASI lub osobę wyznaczoną przez ASI o ustalonym dla niej loginie i konieczności posługiwania się hasłami.
2. Bez spełnienia wymogów wynikających z postanowień § 14 ASI nie może zarejestrować jakiejkolwiek osoby w systemie informatycznym.

§ 18

1. Użytkownik jest wyrejestrowywany z systemu informatycznego w każdym przypadku utraty przez niego uprawnień do dostępu do danych osobowych, co ma miejsce w przypadku:
   - ustania zatrudnienia tego użytkownika w SPZOZ - o czym informacje ASI uzyskuje od pracownika kadrowego, bądź IOD
   - zmiany zakresu obowiązków tego użytkownika – o czym informację ASI uzyskuje od bezpośredniego przełożonego użytkownika.
2. Poza przypadkami wskazanymi w ust. 1 użytkownik jest wyrejestrowywany z systemu informatycznego w każdym przypadku odwołania przez ADO wydanego temu użytkownikowi upoważnienia.

§ 19

W przypadkach wskazanych w §18 co do użytkownika, który utracił uprawnienia dostępu do systemu informatycznego, ASI lub osoba wyznaczona przez ASI niezwłocznie:

1) blokuje jego profil, co powoduje, że osoba ta nie ma możliwości „zalogowania się" do systemu, sieci lub aplikacji;
2) podejmuje inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych osobowych w SPZOZ.

§ 20

Login, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.

ROZDZIAŁ V
PROCEDURY ROZPOCZĘCIA I ZAKOŃCZENIA PRACY

§ 21

Przed przystąpieniem do pracy w systemie użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych służących do przetwarzania danych osobowych oraz dokonać oględzin swojego

stanowiska pracy, ze szczególnym uwzględnieniem czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

§ 22

1. Każdy użytkownik rozpoczynając pracę obowiązany jest „zalogować się" do systemu komputerowego posługując się swoim loginem i hasłem, dokładając jednocześnie szczególnej staranności w tym, aby przy tych czynnościach osoby trzecie nie powzięły wiadomości o treści używanego przez niego hasła. Następnie po podaniu prawidłowego hasła użytkownik ma możliwość „zalogowania się" do aplikacji zawierających dane osobowe.
2. Bez wykonania procedury opisanej w ust.1 jakakolwiek praca w systemie komputerowym nie jest możliwa.

§ 23

1. Maksymalna ilość prób wprowadzenia hasła przy logowaniu się do systemu wynosi 5 (pięć).
2. Po przekroczeniu liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika.
3. Użytkownik informuje ASI o zablokowaniu dostępu do zbioru danych.
4. ASI ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji, informuje IOD i podejmuje odpowiednie działania.

§ 24

1. W przypadku nieaktywności użytkownika na urządzeniu przez okres dłuższy niż 5 minut automatycznie włączany jest wygaszacz ekranu oraz system jest blokowany.
2. Przed opuszczeniem miejsca pracy, użytkownik obowiązany jest odczekać, aż zaktywizuje się wygaszacz ekranu, samemu zaktywizować wygaszacz lub wylogować się.
3. W przypadku, gdy przerwa w pracy trwa dłuższy okres oraz kończąc pracę, użytkownik obowiązany jest „wylogować się" z aplikacji i systemu komputerowego oraz sprawdzić, czy zostały zabezpieczone nośniki informacji.
4. Opuszczając stanowisko pracy użytkownik zamyka pomieszczenia, w których przetwarzane są dane osobowe i przechowywane są nośniki informacji.

§ 25

W przypadku zauważenia przez użytkownika naruszenia zabezpieczenia systemu informatycznego, podejrzenia, że stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń danych osobowych, użytkownik obowiązany jest niezwłocznie poinformować o tym fakcie swojego przełożonego.

ROZDZIAŁ VI
METODA I CZĘSTOTLIWOŚĆ TWORZENIA KOPII AWARYJNYCH ORAZ POSTĘPOWANIE Z NOŚNIKAMI INFORMACJI

§ 26

Tworzenie, przechowywanie i likwidację kopii bezpieczeństwa, regulują szczegółowe instrukcje operacyjne dla poszczególnych aplikacji i systemów przetwarzania oraz odpowiednie akty prawne, w zależności od specyfiki dokumentu, a odnotowywane jest w rejestrze nośników komputerowych zawierających dane osobowe (zał. nr 2).

§ 27

Wydruki komputerowe z systemu zawierające dane osobowe są:

1. Sporządzane tylko dla celów operacyjnych.
2. Odpowiednio opisane i oznakowane.
3. Elementem archiwum bądź składnicy akt w formie papierowej i podlegają zasadom określonym w odpowiednich procedurach.
4. Przechowywane w odpowiednich szafach i używane do celów operacyjnych przez określony czas wykorzystania.

§ 28

Administrator Systemu Informatycznego lub osoba przez niego wyznaczona zobowiązani są do przestrzegania terminów sporządzania kopii zapasowych.

§ 29

Kopie awaryjne są:

1) tworzone na odpowiednio opisanych i oznakowanych nośnikach danych,
2) przechowywane w innych pomieszczeniach niż zbiory danych osobowych eksploatowanych na bieżąco,
3) przechowywane w miejscu, do którego dostęp mogą mieć wyłącznie osoby upoważnione przez ADO.

§ 30

1. Kopiowanie danych osobowych na nośniki informacji i wykonywanie wydruków tych danych jest zabronione, chyba że konieczność sporządzenia wynika z nałożonego na użytkownika zakresu obowiązków i jest uzasadniona potrzebą ich wykonania oraz dozwolona przepisami prawa.
2. Wykorzystywanie nośników informacji lub wydruków w innym celu niż wskazany w ust.1 jest zabronione.

§ 31

1. Częstotliwość tworzenia kopii zapasowych oraz okres ich przechowywania ustala IOD.
2. Kopie zapasowe po ustaniu ich użyteczności są bezzwłocznie usuwane lub niszczone.
3. Kopie zapasowe, które uległy uszkodzeniu podlegają natychmiastowemu zniszczeniu.
4. Niszczenia kopii zapasowych na nośnikach danych dokonuje ASI lub inna upoważniona przez niego osoba.
5. Z nośników danych dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku, gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym dostęp do zawartych na nich danych.
6. Z nośników podlegających zniszczeniu nie wolno sporządzać wydruków.
7. Jeżeli dysk twardy jest uszkodzony i nie ma możliwości skasowania z niego danych osobowych należy wymontować go z komputera i fizycznie zniszczyć.
8. Likwidacji wydruków papierowych dokonuje się przy użyciu przeznaczonych do tego celu mechanicznych niszczarek.
9. Urządzenia, dyski lub inne informatyczne nośniki informacji, 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 jej odczytanie, czego dokonać można w szczególności przez ich trwałe mechaniczne zniszczenie.
10. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie.
11. Trwałego zniszczenia zbędnych nośników i wydruków komputerowych dokonuje się na bieżąco w czasie pracy, nie później jednak niż przed opuszczeniem stanowiska pracy.
12. Dział Informatyczny ma prawo okresowych przeglądów zawartości nośników danych, a w przypadku wykrycia zagrożeń, wpływających na naruszenie ochrony danych osobowych, ma prawo formatowania nośnika łącznie z powiadomieniem o tym fakcie IOD.

ROZDZIAŁ VII
ZASADY UŻYTKOWANIA I ZARZĄDZANIA OPROGRAMOWANIEM

§ 32

1. O zakupie oprogramowania decyduje Dyrekcja SPZOZ, na wniosek ASI i w uzgodnieniu z IOD.
2. Zakupy oprogramowania standardowych systemów operacyjnych, ochrony antywirusowej, edytorów, itp. dotyczą wyłącznie oprogramowania licencjonowanego i mogą być dokonywane włącznie w firmach posiadających uprawnienia na ich dystrybucję.
3. Zakup specjalistycznego oprogramowania dotyczy wyłącznie oprogramowania licencjonowanego i może być dokonywane wyłącznie w firmach informatycznych posiadających stosowne uprawnienia związanych z SPZOZ odpowiednimi umowami o współpracy.

4. Zakupione dla potrzeb SPZOZ oprogramowanie może być wykorzystywane tylko zgodnie z umowami licencyjnymi i serwisowymi.
5. Nie dopuszczalne jest korzystanie w SPZOZ z oprogramowania nielicencjonowanego tzw. oprogramowania pirackiego.
6. Nie dopuszczalne jest wprowadzanie zmian w konfiguracji stacji roboczych oraz instalowanie jakiegokolwiek oprogramowania przez użytkowników.
7. Dział Informatyczny prowadzi wykaz (rejestr) oprogramowania komputerowego (zał. nr 3) nabytego i funkcjonującego w SPZOZ.
8. Instalację oprogramowania na stacjach roboczych może dokonywać tylko pracownik Działu Informatycznego.
9. Za właściwą instalację systemów i oprogramowania na serwerach SPZOZ odpowiedzialny jest ASI i IOD.
10. Za instalację na swoich stanowiskach oprogramowania nielicencjonowanego niezgodnie z postanowieniami Polityki i bez wiedzy ASI odpowiedzialni są poszczególni użytkownicy tych stanowisk.
11. W przypadku wykrycia na stanowisku komputerowym użytkownika wprowadzenia zmian w konfiguracji, oprogramowania nielicencjonowanego, a tym samym naruszenia postanowień Polityki, Dział Informatyczny ma prawo natychmiastowo zabrać stację roboczą w celu przywrócenia właściwych ustawień i stanu oprogramowania.

ROZDZIAŁ VIII
METODA I CZĘSTOTLIWOŚĆ SPRAWDZANIA OBECNOŚCI WIRUSÓW KOMPUTEROWYCH ORAZ METODA ICH USUWANIA

§ 33

Na bieżące i bezpośrednie sprawdzanie obecności wirusów komputerowych pozwala oprogramowanie automatycznie monitorujące występowanie wirusów w trakcie pracy stacji roboczych, wczytywania danych z zewnętrznych nośników informacji lub poprzez sieć wewnętrzną SPZOZ.

§ 34

1. Nadzór nad instalowaniem nowego oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje ASI lub osoba przez niego wyznaczona.
2. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach danych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
3. Oprogramowanie antywirusowe musi być systematycznie uaktualniane.

§ 35

1. Po każdorazowym wykryciu wirusa przez oprogramowanie monitorujące użytkownik obowiązany jest niezwłocznie poinformować swojego przełożonego oraz ASI.
2. W razie niemożliwości usunięcia wirusa, ASI ma obowiązek niezwłocznego przedstawienia IOD lub ADO propozycji działań zaradczych.
3. W sytuacji korzystania z usług specjalistów zewnętrznych należy podjąć działania uniemożliwiające tym osobom dostęp do danych osobowych. Osoby te mogą dokonywać operacji na „zainfekowanym" komputerze wyłącznie pod opieką ASI lub upoważnionej przez niego osoby.

§ 36

1. Po usunięciu wirusa ASI sprawdza system informatyczny oraz przywraca go do pełnej funkcjonalności i sprawności.
2. ASI, jeżeli zachodzi taka konieczność – wnioskuje do ADO o zakup nowego programu antywirusowego.
3. ASI rejestruje wszystkie przypadki zainfekowania komputerów i nośników wykorzystywanych do przetwarzania danych osobowych w dzienniku (zał. nr 1).
4. Procedura przedstawiona powyżej ma również zastosowanie do przypadków awarii systemu spowodowanych błędem programu bądź użytkowników.

ROZDZIAŁ IX
WYMAGANIA SPRZĘTOWO-ORGANIZACYJNE W ZAKRESIE OCHRONY

PRZETWARZANYCH DANYCH OSOBOWYCH

§ 37

Sprzęt obsługujący zbiory danych osobowych SPZOZ w Parczewie składa się z komputerów stacjonarnych klasy PC i terminali, zlokalizowanych w wydzielonych pomieszczeniach SPZOZ. Nie zezwala się na trwałe przechowywanie tych zbiorów na komputerach przenośnych, używanych poza terenem SPZOZ.

§ 38

1. Prowadzone i obsługiwane przez SPZOZ bazy danych osobowych przetwarzane są na serwerze lub na stacji lokalnej.
2. Pomieszczenie stacji lokalnej powinno wykluczać dostęp osób nieuprawnionych.
3. Serwer lub stacja lokalna z bazą danych przetwarzające dane osobowe w zbiorze danych powinny być zabezpieczone zasilaczem awaryjnym o mocy umożliwiającej podtrzymanie napięcia minimum 15 minut. Jeśli jednostka pracuje przez całą dobę, zasilacz powinien zawierać oprogramowanie do automatycznego wyłączenia urządzenia w przypadku przekroczenia czasu podtrzymania zasilania z automatycznym, bezpiecznym wyłączeniem bazy danych osobowych.

§ 39

1. Ekrany monitorów powinny być ustawione do wewnątrz pomieszczeń wydzielonych do przetwarzania danych osobowych, w taki sposób, by uniemożliwić wgląd lub spisanie zawartości aktualnie wyświetlanej na ekranie monitora.
2. Programy zainstalowane na komputerach stacjonarnych i przenośnych obsługujących przetwarzanie danych osobowych użytkowane są z zachowaniem praw autorskich i posiadają licencje.
3. Decyzję o instalacji oprogramowania systemowego oraz oprogramowania użytkowego obsługującego przetwarzanie danych osobowych, po zasięgnięciu opinii IOD podejmuje ASI.
4. Używanie przez użytkownika sprzętu komputerowego przeznaczonego do przetwarzania danych osobowych do innych celów niż określone w zakresie obowiązków, jest zabronione.

§ 40

1. Drzwi wejściowe do budynku i pomieszczeń, w których przetwarzane są dane osobowe powinny być zabezpieczone.
2. Pomieszczenia serwerowni zabezpieczone są drzwiami przeciwpożarowymi z zainstalowanym systemem kontroli dostępu oraz wyposażone w sprzęt gaśniczy przeznaczony dla urządzeń elektronicznych.
3. Wejście do serwerowni mają tylko osoby upoważnione: ASI, a razem z nim: ADO, IOD, a w przypadku awarii, konserwacji, konieczności przeprowadzenia aktualizacji, modernizacji itp. serwisanci zewnętrzni.

§ 41

1. Stały dostęp do pomieszczeń SPZOZ mają tylko użytkownicy oraz pracownicy obsługi.
2. Osoby trzecie mogą przebywać w tych pomieszczeniach wyłącznie w obecności co najmniej jednego upoważnionego użytkownika.
3. W trakcie prac technicznych wykonywanych przez osoby trzecie, przetwarzanie danych na wydzielonych stanowiskach jest zabronione, a sprzęt komputerowy musi być wyłączony.

§ 42

Przeglądy i konserwacje sprzętu komputerowego dokonuje się w miarę potrzeb wynikających z obciążenia sprzętu komputerowego, warunków zewnętrznych, w których pracują dane urządzenia oraz priorytetu danego sprzętu dla funkcjonowania całości systemu informatycznego.

§ 43

1. Prace dotyczące przeglądów, konserwacji i napraw wymagające autoryzowanych firm zewnętrznych, są wykonywane przez uprawnionych przedstawicieli tych firm (serwisantów) pod nadzorem ASI lub upoważnionej przez niego osoby, bez możliwości dostępu do danych osobowych.
2. W wypadku konieczności dostępu do danych osobowych przez serwisantów, podpisują oni dokument o zachowaniu poufności.
3. Urządzenia, dyski lub inne informatyczne nośniki informacji przeznaczone do napraw, gdzie wymagane jest zaangażowanie autoryzowanych podmiotów zewnętrznych, pozbawia się przed naprawą zapisu tych danych albo naprawia się pod nadzorem ASI lub osoby przez niego upoważnionej.

ROZDZIAŁ X
SPOSÓB POSTĘPOWANIA W ZAKRESIE KOMUNIKACJI W SIECI KOMPUTEROWEJ
§ 44

1. Komunikacja w sieci komputerowej jest dozwolona jedynie po właściwym zalogowaniu się i podaniu hasła użytkownika.
2. Wprowadzanie do systemu informatycznego informacji z zewnątrz, w tym danych osobowych, jest dopuszczalne tylko przy stwierdzeniu legalności i wiarygodności źródeł informacji i tylko przez użytkownika w zakresie jego obowiązków i wynikających z nich uprawnień.
3. Konfiguracja systemu informatycznego i sieci jest dokonywana wyłącznie przez ASI lub upoważnione przez niego osoby.
4. W celu uniemożliwienia niekontrolowanej wymiany informacji, w tym danych osobowych lub modyfikacji systemu informatycznego wymagana jest odpowiednia konfiguracja komputerowych stanowisk pracy.
5. Niedozwolone jest podłączanie prywatnych urządzeń do sieci komputerowej SPZOZ, z wyjątkiem wydzielonej bezprzewodowej sieci w postaci punktów dostępowych hotspot na oddziałach.
6. Pliki zawierające dane osobowe powinny znajdować się jedynie na wydzielonych komputerach, gdzie podlegają ochronie zapewnianej przez mechanizmy bezpieczeństwa systemu operacyjnego (np. uwierzytelnianie).
7. Na stacjach roboczych użytkowników dane osobowe nie powinny być przechowywane, z wyjątkiem pracy jednostanowiskowej, bez wykorzystania serwerów i sieci.
8. Nieuzasadnione kopiowanie przez użytkowników plików z serwerów na stacje robocze i inne nośniki jest zabronione.
9. Wszelkie pliki z danymi osobowymi przesyłane na zewnątrz SPZOZ przez łącza publiczne muszą być zaszyfrowane bądź chronione hasłem lub przesyłane przy pomocy bezpiecznego protokołu HTTPS.
10. Komunikacja między klientami (użytkownikami) łączącymi się z systemem przez Internet za pomocą Serwera WWW odbywa się przy pomocy bezpiecznego protokołu HTTPS.
11. Komunikacja użytkowników łączących się z siecią szpitalną i systemem przez Internet odbywa się za pomocą dedykowanego tunelu SSL VPN.

ROZDZIAŁ XI
ZASADY KORZYSTANIA Z KOMPUTERÓW PRZENOŚNYCH
§ 45

1. Komputery przenośne, używane do przetwarzania danych osobowych, powinny być zabezpieczone podczas transportu oraz przechowywania przed dostępem do tych danych osób nieuprawnionych.
2. W szczególności należy:
   - Zabezpieczyć dostęp do komputera hasłem,
   - Nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych,
   - Nie zezwalać na wynoszenie komputerów zawierających dane poza teren SPZOZ w Parczewie,
   - Pliki z danymi osobowymi należy zaszyfrować bądź chronić hasłem.

ROZDZIAŁ XII
POSTĘPOWANIE W PRZYPADKU NARUSZENIA ZABEZPIECZENIA SYSTEMU OCHRONY DANYCH OSOBOWYCH
§ 46

1. Do czasu przybycia IOD, zgłaszający:
   - Informuje ASI i zabezpiecza dostęp do miejsca naruszenia ochrony lub urządzenia przez osoby trzecie,
   - wstrzymuje pracę na urządzeniu, na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby stacji roboczych i innych urządzeń, które w związku z naruszeniem ochrony zostały wstrzymane, a w szczególności odcina zewnętrzną sieć przesyłania danych (np. Internet)
   - nie zmienia położenia przedmiotów, które pozwalają stwierdzić naruszenie ochrony lub odtworzyć jego okoliczności,

- podejmuje, stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

2. Zgodę na uruchomienie stacji roboczej i innych urządzeń wyraża ASI.
3. Po zaistnieniu okoliczności wskazującym na naruszenie ochrony, osoba zatrudniona przy przetwarzaniu danych osobowych może kontynuować prace dopiero po otrzymaniu zgody IOD.
4. Dokonywanie zmian w miejscu naruszenia ochrony bez uzyskania zgody, o której mowa w pkt 3 jest dopuszczalne, jeżeli chodzi o konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.
5. Okoliczności i przyczyny naruszeń ochrony ustala zespół, w którego skład wchodzi IOD, ASI oraz pracownik ze stanowiska pracy, na którym nastąpiło naruszenie ochrony.
6. Niezwłocznie po otrzymaniu wiadomości o naruszeniu ochrony zespół, o którym mowa w pkt 5, przystępuje do ustalenia okoliczności i przyczyn tego naruszenia, a w szczególności:
   - dokonuje oględzin miejsca naruszenia bądź urządzenia, w którym wykryto naruszenie oraz bada inne okoliczności, które mogły mieć wpływ na powstanie naruszenia ochrony;
   - wysłuchuje opinii osoby zatrudnionej przy przetwarzaniu danych osobowych, która dokonała powiadomienia;
   - jeżeli jest to potrzebne sporządza szkic, fotografię miejsca naruszenia ochrony;
   - podejmuje decyzję o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych i w przypadkach uzasadnionych niezwłocznie powiadamia Administratora Danych;
7. Zespół, o którym mowa w pkt 5 sporządza protokół oględzin, który stanowi podstawę do:
   - ustalenia skali stwierdzonych naruszeń ochrony, przyczyn ich powstania, skutków, jakie wywołują lub mogą wywołać, w odniesieniu do stanu zabezpieczenia danych osobowych lub ich zbiorów w SPZOZ;
   - wyciągnięcia wniosków, zwłaszcza co do podjęcia określonych działań organizacyjnych i technicznych.
8. Protokół oględzin, o którym mowa w pkt 7 zespół przedstawia ADO, który podejmuje decyzję o koniecznych działaniach organizacyjnych i technicznych.
9. IOD w przypadkach określonych w Polityce podejmuje kroki zmierzające do likwidacji naruszeń ochrony i zapobieżenia wystąpieniu ich w przyszłości.
10. W tym celu:
    - w miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu;
    - przedstawia na bieżąco ADO informację o podjętych czynnościach;
    - jeśli zachodzi potrzeba, przedstawia propozycję wprowadzenia nowych form zabezpieczenia systemu, a w razie ich wprowadzenia zaznajamia z nimi osoby zatrudnione przy przetwarzaniu danych.

ROZDZIAŁ XIII
POSTANOWIENIA KOŃCOWE

§ 47

Osoba zatrudniona przy przetwarzaniu danych osobowych za naruszenie obowiązków wynikających z niniejszej Polityki i przepisów Rozporządzenia o ochronie danych ponosi odpowiedzialność przewidzianą w Kodeksie Pracy oraz wynikającą z ustawy, o której mowa.

§ 48

W sprawach nie uregulowanych Polityką zastosowanie mają przepisy rozporządzenia o ochronie danych (RODO), ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Niniejsza instrukcja wchodzi w życie z dniem jej podpisania przez Dyrektora SPZOZ.

Załączniki:

1. Dziennik systemu
2. Rejestr nośników komputerowych zawierających dane osobowe
3. Wykaz oprogramowania komputerowego
4. Dziennik wizyt w serwerowni

Parczew, dnia 01.02.2021 r.

Sporządził
Kierownik Działu Informatycznego

mgr inż. Paweł Korszeń
Podpis nieczytelny

Zatwierdził
p.o. Dyrektora SPZOZ W Parczewie

mgr inż. Ryszard Kielar
Podpis nieczytelny

ROZDZIELNIK: Polityka **Zarządzanie Systemem Informatycznym**
Wydanie 03 z dnia 01.02.2021 r.

Lp.	**Dokument**	**Kto otrzymuje**	**Data**	**Podpis**
1.	Oryginał	Pełnomocnik ds. ZSZ	02.02.2021 r.	
2.	Kopia nr 1	ZKZSz	02.02.2021 r.	Wersja elektroniczna
3.	Kopia nr 2	OIT	02.02.2021 r.	Wersja elektroniczna
4.	Kopia nr 3	SOR	02.02.2021 r.	Wersja elektroniczna
5.	Kopia nr 4	Blok operacyjny	02.02.2021 r.	Wersja elektroniczna
6.	Kopia nr 5	O/ internistyczno – kardiologiczny	02.02.2021 r.	Wersja elektroniczna
7.	Kopia nr 6	O/ ginekologiczno – położniczy	02.02.2021 r.	Wersja elektroniczna
8.	Kopia nr 7	O/ chirurgiczny	02.02.2021 r.	Wersja elektroniczna
9.	Kopia nr 8	O/ dziecięcy	02.02.2021 r.	Wersja elektroniczna
10.	Kopia nr 9	O/ geriatryczny	02.02.2021 r.	Wersja elektroniczna
11.	Kopia nr 10	O/ psychiatryczny	02.02.2021 r.	Wersja elektroniczna
12.	Kopia nr 11	O/ rehabilitacyjny	02.02.2021 r.	Wersja elektroniczna
13.	Kopia nr 12	Zespół Poradni specjalistycznych	02.02.2021 r.	Wersja elektroniczna
14.	Kopia nr 13	Dział rehabilitacji	02.02.2021 r.	Wersja elektroniczna
15.	Kopia nr 14	Pracownia diagnostyki obrazowej	02.02.2021 r.	Wersja elektroniczna
16.	Kopia nr 15	Pracownia endoskopowa	02.02.2021 r.	Wersja elektroniczna
17.	Kopia nr 16	Dział zatrudnienia i płac	02.02.2021 r.	Wersja elektroniczna
18.	Kopia nr 17	Dział finansowo- księgowy	02.02.2021 r.	Wersja elektroniczna
19.	Kopia nr 18	Dział zamówień publicznych	02.02.2021 r.	Wersja elektroniczna
20.	Kopia nr 19	Dział metodyczno – organizacyjny	02.02.2021 r.	Wersja elektroniczna
21.	Kopia nr 20	Inspektor ds. bhp	02.02.2021 r.	Wersja elektroniczna

22.	Kopia nr 21	Inspektor OC	02.02.2021 r.	Wersja elektroniczna
23.	Kopia nr 22	Kuchnia	02.02.2021 r.	Wersja elektroniczna
24.	Kopia nr 23	Sterylizatornia	02.02.2021 r.	Wersja elektroniczna
25.	Kopia nr 24	Apteka szpitalna	02.02.2021 r.	Wersja elektroniczna
26.	Kopia nr 25	Dział informatyczny	02.02.2021 r.	Wersja elektroniczna
27.	Kopia nr 26	Dział utrzymania ruchu i gospodarczy	02.02.2021 r.	Wersja elektroniczna
28.				
29.				
30.				