ZATWIERDZIŁ

PREZES ZARZĄDU
ARTIMED NZOZ Sp. z o.o.

lek. med. Dariusz Saletra

V-ce Prezes Zarządu

lek. med. Iwona Saletra

POLITYKA BEZPIECZEŃSTWA

PRZETWARZANIA DANYCH OSOBOWYCH

---

w ARTIMED NZOZ Sp. z o.o.

z siedzibą ul. Paderewskiego 4B, 25-017 Kielce

SPIS TREŚCI

ROZDZIAŁ I
Postanowienia ogólne

1. Polityka Bezpieczeństwa przetwarzania Danych Osobowych w Artimed NZOZ Sp. z o.o. z siedzibą w Kielcach, zwana dalej także „Polityką" lub „Polityką Bezpieczeństwa", została wydana w związku z Ustawą o ochronie Danych Osobowych.
2. Celem niniejszej Polityki jest stworzenie podstawy dla metod zarządzania i wymagań niezbędnych dla zapewnienia w Artimed NZOZ Sp. z o.o. (dalej: „Spółka") odpowiedniego do zagrożeń poziomu ochrony Danych Osobowych, na każdym etapie ich przetwarzania. Polityka określa środki techniczne i organizacyjne niezbędne do zachowania integralności, poufności i rozliczalności przetwarzanych danych osobowych.
3. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów:
    1) Poufność danych – rozumianą jako właściwość zapewniającą, że Dane nie są udostępniane nieupoważnionym osobom.
    2) Integralność danych – rozumianą jako właściwość zapewniającą, że Dane Osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
    3) Rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny.
    4) Integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzone, jak i przypadkowej.
4. Definicje użyte w Polityce:
    1) **Administrator Danych** – Artimed NZOZ Sp. z o.o. w Kielcach ul. Paderewskiego 4B
    2) **Administrator Systemu Informatycznego (ASI)** – osoba odpowiedzialna za realizację zadań związanych z prawidłowym funkcjonowaniem systemu
    3) **Aplikacja** – programowa część Systemu Informatycznego, realizująca funkcję gromadzenia i przetwarzania danych,
    4) **Dane** - informacje zapisywane w zbiorach lub bazach danych przez aplikacje informatyczne,
    5) **Dane Osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, przetwarzane przez administratora danych zarówno w Systemach Informatycznych jak i tradycyjnie (wersja papierowa).
    6) **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie Użytkownikowi.
    7) **Identyfikator** – unikalna nazwa Użytkownika rozpoznawana przez System Informatyczny,
    8) **Informacja medyczna i dokumentacja medyczna** - są to informacje dotyczące stanu zdrowia pacjentów, przetwarzane zgodnie z wymaganiami ustawy z dnia 6 listopada z 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2016, poz. 186) i rozporządzenia Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów i wzorów zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z 2015 r. poz. 2069),
    9) **Infrastruktura Informatyczna** – sprzęt komputerowy, urządzenia sieciowe, systemy operacyjne, oprogramowanie systemowe.
    10) **Inspektor Ochrony Danych (IOD)** – osoba powołana przez Administratora Danych zgodnie z art. 37 RODO.
    11) **Integralność** – zagwarantowanie kompletności i aktualności danych.
    12) **Kartoteka** – zbiory danych przetwarzane w formie papierowej.
    13) **Kierownik jednostki organizacyjnej** – osoba odpowiedzialna za skuteczne funkcjonowanie danego obszaru działalności Spółki, realizująca bieżący nadzór nad tym obszarem, zgodnie z zakresem kompetencji określonym w Regulaminie Organizacyjnym Spółki lub zadaniami przypisanymi do zakresu działania danej komórki.
    14) **Nośniki** – wszelkie nośniki, na których informacje zapisane są w postaci elektronicznej, w szczególności dyski, płyty CD/DVD, pamięci przenośne.
    15) **Poufność** – właściwość systemu uniemożliwiająca dostęp do jego zasobów osobom nieupoważnionym.
    16) **Pracownik** – rozumie się przez to osobę wykonującą określonego rodzaju pracę na rzecz Artimed NZOZ Sp. z o.o. na podstawie umowy o pracę, umowy o dzieło lub umowy zlecenie.

17) **Prezes** - rozumie się przez to Prezesa Zarządu Artimed NZOZ Sp. z o.o.
18) **Przetwarzanie Danych Osobowych** – jakiekolwiek operacje wykonywane na Danych Osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie Danych Osobowych, w szczególności w Systemach Informatycznych.
19) **Rozporządzenie (RODO)** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem Danych Osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
20) **System Informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
21) **Ustawa** – Ustawa o ochronie Danych Osobowych.
22) **Użytkownik** – osoba upoważniona do dostępu do zasobów papierowych oraz Systemu Informatycznego posiadająca upoważnienie do przetwarzania Danych Osobowych w tym systemie.
23) **Wirus** – nieautoryzowany program inwazyjny, powodujący zakłócenia pracy Systemu Informatycznego.
24) **Współpracownik** – osoba fizyczna, bądź prawna, która na podstawie stosownej umowy wykonuje na rzecz Spółki Artimed NZOZ określoną usługę.
25) **Zbiór Danych Osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

ROZDZIAŁ II
Zakres i cel Polityki Bezpieczeństwa

1. Politykę Bezpieczeństwa stosuje się do Danych Osobowych przetwarzanych przez Administratora Danych w Systemie Informatycznym oraz dokumentacji wytworzonej metodą tradycyjną (papierową). W szczególności do Danych Osobowych obejmujących informacje medyczne i dokumentację medyczną, które są zasobami szczególnie chronionymi.
2. Politykę Bezpieczeństwa stosuje się do Danych Osobowych przetwarzanych zarówno w przypadku, gdy Artimed NZOZ Sp. z o.o. jest Administratorem Danych, jak i w sytuacji, gdy przetwarza dane na podstawie umów powierzenia w trybie art. 28 RODO.
3. Celem Polityki Bezpieczeństwa jest określenie kierunków działań oraz wsparcia dla zapewnienia bezpieczeństwa przetwarzania Danych Osobowych w celu prawidłowej ochrony przetwarzanych Danych Osobowych.
4. W zakresie podmiotowym Polityka obowiązuje wszystkich pracowników Administratora Danych oraz inne osoby mające dostęp do Danych Osobowych.
5. Polityka odnosi się do wszystkich Nośników informacji, na których są lub będą znajdować się Dane Osobowe podlegające ochronie.
6. Polityka odnosi się wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane Dane Osobowe podlegające ochronie.
7. Zarząd deklaruje zaangażowanie swoje i Kierowników komórek organizacyjnych w ustanowienie, skuteczne wdrożenie i ciągłe doskonalenie celów Administratora Danych w zakresie bezpieczeństwa informacji oraz w przestrzeganie zasad bezpieczeństwa informacji. Cele te i spełnienie obowiązujących wymagań w zakresie bezpieczeństwa informacji są integralną częścią strategii działania Artimed NZOZ Sp. z o.o.
8. Cele funkcjonującego w Spółce Artimed NZOZ systemu bezpieczeństwem informacji dotyczą w szczególności:
    1) Spełnienia wymagań prawnych w zakresie ochrony Danych Osobowych.
    2) Ochrony informacji o stanie zdrowia Pacjentów.

3) Zapewnienia skutecznych zabezpieczeń Danych Osobowych, zarówno w Systemach Informatycznych, jak i poza nimi.
4) Propagowania wiedzy o zasadach bezpiecznego przetwarzania Danych Osobowych przez pracowników, współpracowników i kontrahentów Spółki Artimed NZOZ

9. Wykaz dokumentów powiązanych z polityką bezpieczeństwa danych określających procedur oraz zasad bezpieczeństwa jest prowadzony przez Inspektora Ochrony Danych.

ROZDZIAŁ III
Jednostki zaangażowane w realizację polityki oraz struktura zarządzania ryzykiem

1. Zarząd Spółki:
   1) Zatwierdza postanowienia niniejszej Polityki Bezpieczeństwa.
   2) Ustala strategie i wykorzystanie zasobów w celu realizacji zadań dotyczących ochrony Danych Osobowych.
   3) Powołuje Inspektora Ochrony Danych (IOD), który nadzoruje w Spółce przestrzeganie zasad ochrony Danych Osobowych określonych w Polityce Bezpieczeństwa oraz w dokumentach z nimi związanych.
   4) Powołuje Administratora Systemu Informatycznego (ASI), który administruje zasobami sprzętowo-programowymi służącymi do przetwarzania Danych Osobowych.
2. Inspektor Ochrony Danych:
   1) Informuje Administratora Danych, podmiot przetwarzający oraz pracowników, którzy przetwarzają Dane Osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradza im w tej sprawie.
   2) Monitoruje przestrzeganie Rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony Danych Osobowych, w tym podział obowiązków, działania zwiększające świadomość, przeprowadzanie szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.
   3) Współpracuje z organem nadzorczym (UODO).
   4) Udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art.35 RODO.
   5) Pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym uprzednimi konsultacjami, o których mowa w art.36 Rozporządzenia oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
   6) Nadzoruje prowadzenie rejestru czynności przetwarzania danych oobowych.
   7) Wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
3. Administratora Systemu Informatycznego:
   1) Sprawuje nadzór nad prawidłową eksploatacją Systemów Informatycznych, zgodnie z celami przetwarzania w nich Danych Osobowych poprzez:
      a) Opracowanie instrukcji nadawania, modyfikacji i odbierania uprawnień do Systemów Informatycznych.
      b) Nadzorowanie dostępu do Systemów Informatycznych służących do przetwarzania Danych Osobowych i raportowanie wyników tego nadzoru do IOD.
      c) Prowadzenie konserwacji oprogramowania.
      d) Zapewnienie ochrony nośników zawierających kopie zbiorów Danych Osobowych.
   2) Realizuje wytyczne IOD w zakresie ochrony Danych Osobowych przetwarzanych z wykorzystaniem środków informatycznych.
   3) Informuje IOD i Administratora Danych o incydentach i wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu ochrony Danych Osobowych.
4. Wszyscy Użytkownicy:

1) Przestrzegają zasad ochrony Danych Osobowych określonych w niniejszej Polityce Bezpieczeństwa.
2) Zapoznają się z obowiązującymi wymaganiami, w tym przepisami prawa w zakresie ochrony Danych Osobowych.
3) Przetwarzają Dane Osobowe zgodnie z celem i zakresem przetwarzania.
4) Informują IOD o incydentach i o wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu ochrony Danych Osobowych.
5) Zapewniają Poufność Danych Osobowych, do których uzyskują dostęp.
6) Przestrzegają zasady czystego ekranu, dbają o bezpieczeństwo stanowiska pracy, w tym zwłaszcza blokowanie komputera, włączanie wygaszacza ekranu chronionego hasłem lub wylogowanie z systemu przed opuszczaniem stanowiska pracy.
7) Przestrzegają zasady czystego biurka. W przypadku opuszczenia miejsca pracy na biurku nie powinny znajdować się żadne dokumenty służbowe.
8) Przestrzegają zasady czystej drukarki / kserokopiarki / skanera. Wszystkie dokumenty drukowane / kserowane / skanowane należy zabrać z urządzenia.
9) Wykazują ostrożność przy odbieraniu poczty elektronicznej przychodzącej od nieznanych adresatów lub o podejrzanym tytule e-maila.
10) Dbają o to, by dokumenty były przechowywane w zamkniętych sejfach, szafach lub szufladach.
11) Zapewniają ochronę używanych przez siebie komputerów przenośnych oraz innych nośników danych osobowych.
12) Podpisują „Oświadczenie o zachowaniu poufności", które stanowi **załącznik nr 2** do niniejszej Polityki Bezpieczeństwa oraz przestrzegają jego postanowień.

5. Struktura zarządzania ryzykiem:
   1) Podstawowym założeniem procesu zarządzania ryzykiem Artimed NZOZ Sp. z o.o. jest, że realizują go wszyscy Użytkownicy, poprzez postępowanie zgodne z powszechnie obowiązującymi przepisami prawa, wymaganiami korporacyjnymi oraz wewnętrznymi przepisami Spółki (ustanowionymi przez Zarząd regulacjami dot. danego obszaru działania / procesu).
   2) Za skuteczne zarządzanie ryzykiem, odpowiednio w nadzorowanych przez siebie obszarach, odpowiada Kadra Kierownicza poprzez:
      a) Ustalenie celów operacyjnych dla nadzorowanego obszaru, a w przypadku odchylenia w realizacji danego celu - przedstawienie propozycji rozwiązania do decyzji Zarządu.
      b) Identyfikację zdarzeń/okoliczności, które mogły mieć wpływ na osiągnięcie postawionych celów lub ich zmianę.
      c) Analizowanie wpływu oraz prawdopodobieństwa wystąpienia zdarzeń, które mogą negatywnie oddziaływać na realizację postawionych celów.
      d) Zaprojektowanie i efektywne funkcjonowanie działań kontrolnych, adekwatnych do skali działalności w danym obszarze i zapewniających skuteczność nadzoru.
      e) Monitorowanie efektywności funkcjonowania zarządzania ryzykiem w podległym obszarze.
      f) Podejmowanie działań ograniczających ryzyko.
   3) Szacowanie ryzyka jest dokonywane na podstawie dokumentów:
      a) Procedura oceny skutków dla Ochrony Danych.

ROZDZIAŁ IV
Zasady Eksploatacji Infrastruktury Informatycznej

1. Eksploatacja Systemów Informatycznych:
   1) Za przestrzeganie obowiązujących wymagań eksploatacji systemów odpowiedzialne są osoby upoważnione do przetwarzania Danych Osobowych w tych systemach.
   2) Systemy Informatyczne winny być wyposażone w mechanizmy umożliwiające, w czasie wykonywania rutynowych działań, wykrycie błędów.
2. Ochrona przed oprogramowaniem inwazyjnym (wirusami):

1) Program komputerowy służący do przetwarzania Danych Osobowych należy zabezpieczyć przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do programu.
2) Ochrona antywirusowa realizowana jest przez oprogramowanie antywirusowe, które jest instalowane na wszystkich stacjach roboczych oraz systematycznie aktualizowane.
3) W przypadku wykrycia Wirusa należy podjąć następujące działania:
   a) Należy natychmiast zgłosić swojemu przełożonemu, który powiadamia o tym fakcie Administratora Systemu Informatycznego.
   b) Odłączyć od sieci internetowej podejrzane komputery.
   c) Usunąć Wirusa z zainfekowanego komputera.
   d) Przeskanować komputer programem antywirusowym.
   e) Podłączyć kabel do sieci internetowej.
   f) Ponownie przeskanować komputer programem antywirusowym.
   g) Spróbować określić sposób przedostania się Wirusa do sieci.
4) Nie używa się oprogramowania, które uprzednio nie zostało sprawdzone pod kątem aktualności i zasad określonych w przepisach dotyczących przetwarzania Danych Osobowych.
5) Jeżeli zachodzi podejrzenie, że zostały zmodyfikowane pliki systemowe lub pliki zainstalowanych programów należy zainstalować nową kopię systemu.

3. Przekazywanie danych i oprogramowania:
   1) Dane Osobowe są przekazywane poprzez sieć publiczną odbywa się przy użyciu odpowiedniej metody szyfrującej:
      a) Dane są szyfrowane w miejscu ich nadania, a deszyfrowane w miejscu obioru.
      b) Szyfrowanie i deszyfrowanie odbywać się może wyłącznie przy udziale osób upoważnionych.
      c) Zaleca się szyfrowanie z wykorzystaniem algorytmu AES-256.
   2) Dane przesyłane w sposób ciągły poza sieć teleinformatyczną Administratora Danych powinny być wykonywane poprzez zastosowanie bezpiecznego kanału danych VPN.
   3) Pracownicy nie mogą używać do celów służbowych innych skrzynek niż przydzielonych im indywidualnie przez Administratora Systemu.
   4) Przekazywanie/otrzymywanie Danych Osobowych lub oprogramowania wykorzystywanego do przetwarzania Danych Osobowych do/z firmy zewnętrznej powinno odbywać się na podstawie umowy precyzującej warunki zapewniające bezpieczeństwo takiej wymiany.
   5) Hasło musi być przekazane inną drogą niż zastosowana do przesyłki pliku (np. sms, telefonicznie).
4. Eksploatacja przenośnych urządzeń, w których są przetwarzane Dane Osobowe:
   1) Urządzenia przenośne winny być tak skonfigurowane, aby po określonym upływie czasu automatycznie blokować dostęp do swoich zasobów.
   2) Po opuszczeniu miejsca pracy ekran monitora komputera przenośnego winien być domknięty, tak aby umożliwiło to przejście w stan wymuszający ponowne zalogowanie.
   3) Zabronione jest pozostawienie urządzenia przenośnego w miejscu publicznym bez nadzoru i opieki.
   4) Dane Osobowe przetwarzane na komputerach przenośnych powinny być zabezpieczone w sposób zapewniający poufność tych danych, w szczególności Dane te powinny być zabezpieczone metodami kryptograficznymi.
5. Założenia dotyczące użytkowania Systemów Informatycznych:
   1) Systemy Informatyczne stosowane w Artimed NZOZ Sp. z o.o. mogą być wykorzystywane wyłącznie w celach służbowych.
   2) Zasoby Systemu Informatycznego przetwarzane są wyłącznie zgodnie z ich przeznaczeniem.
   3) Ograniczenia podłączania urządzeń do służbowego sprzętu komputerowego urządzenia pamięci przenośnej typu flashpen, pendrive, dysk usb:
      a) Muszą pochodzić z zaopatrzenia wewnętrznego Spółki.

b) Mogą służyć do przechowywania informacji chronionych, pod warunkiem stosowania zabezpieczeń kryptograficznych.

4) Nie można podłączać modemów lub innych urządzeń umożliwiających dostęp do Internetu niepochodzących z zaopatrzenia wewnętrznego Spółki, chyba że IOD wyrazi na to zgodę.
5) Nie wolno korzystać jednocześnie z usług sieci wewnętrznej (LAN) oraz podłączać modemów i innych urządzeń umożliwiających dostęp do Internetu.
6) Kontrola zabezpieczeń Systemów Informatycznych dokonywana jest wyłącznie przez uprawnione osoby.
7) Bezpośrednio przed opuszczeniem stanowiska pracy Użytkownik wyłącza lub blokuje stację roboczą.
8) System Informatyczny umożliwia zalogowanie wyłącznie uprawnionym Użytkownikom (zabrania się używania konta typu "gość").
9) Hasła administracyjne podlegają szczególnej ochronie – za nadzorowanie skuteczności tej ochrony odpowiada ASI.
10) Użytkownicy nie posiadają dostępu do narzędzi administracyjnych systemu.
11) Prawidłowy poziom zabezpieczenia Systemu Informatycznego służącego do przetwarzania Danych Osobowych zostaje zapewniony poprzez przestrzeganie następujących zasad:
    a) Uniemożliwienie osobom postronnym uzyskiwanie nieupoważnionego dostępu
    b) Instalowanie nowego lub aktualizowanie już zainstalowanego oprogramowania wyłącznie przez uprawnionych Użytkowników Systemu Informatycznego,
    c) Niepodejmowanie przez Użytkowników Systemu Informatycznego prób testowania, modyfikacji i naruszenia zabezpieczeń systemu lub jakichkolwiek działań noszących takie znamiona.

6. Założenia dotyczące komunikacji w sieci teleinformatycznej:
    1) Przesyłanie Danych Osobowych drogą teletransmisji powinno odbywać się wyłącznie przy wykorzystaniu wymaganych zabezpieczeń chroniących przed nieuprawnionym dostępem, w szczególności takich jak ochrona kryptograficzna.
    2) Administrator Danych powinien chronić system przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, poprzez:
        a) Kontrolę przepływu informacji pomiędzy systemem informatycznym, a siecią publiczną.
        b) Kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
    3) Kontrola opisana powyżej powinna być dokumentowana przez osoby wykonujące te czynności.

ROZDZIAŁ V
Przetwarzanie danych w Kartotekach papierowych

1. Sposób przechowywania Kartotek:
    1) Kartoteki są przechowywane w sposób uporządkowany.
    2) Dostęp do Kartotek przyznany jest wyłącznie osobom upoważnionym.
    3) Kartoteki należy przechowywać w wyznaczonych do tego celu szafach.
    4) Szafy z chronionymi dokumentami są zamykane na klucz.
    5) Szafy z chronionymi dokumentami znajdują się w pomieszczeniu, do którego mają dostęp tylko osoby upoważnione.
    6) Klucze od szaf z dokumentami zawierającymi Dane Osobowe są przechowywane w taki sposób, aby osoby postronne nie miały do nich dostępu.
2. Zasady obiegu dokumentów papierowych i wynoszenia ich poza obszar przetwarzania to:
    1) Dokumenty papierowe nie mogą być, bez istotnej przyczyny, wynoszone poza obszar przetwarzania.
    2) Przed wyniesieniem dokumentacji poza obszar przetwarzania należy poinformować bezpośredniego przełożonego i uzyskać jego zgodę.

3. Niepotrzebne wydruki lub inne dokumenty należy niszczyć w niszczarkach lub wrzucać do pojemników przeznaczonych do tego celu.

ROZDZIAŁ VI
Zarządzanie ochroną Danych Osobowych

1. Administrator Danych zabezpiecza Dane Osobowe przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy o ochronie Danych Osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy, zasady określone w niniejszej Polityce oraz w dokumentach powiązanych powinny być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez Współpracowników Administratora Danych.
3. Wszystkie osoby wytypowane do przetwarzania Danych Osobowych, przed dopuszczeniem do danych, winny być przeszkolone w zakresie ochrony Danych Osobowych.
4. Za przeprowadzenie szkolenia z ochrony Danych Osobowych odpowiada Administrator Danych. Harmonogram szkoleń w tym zakresie ustala IOD, w porozumieniu z Zespołem Zarządzania Kadrami Spółki Artimed NZOZ.
5. Kierownicy jednostek organizacyjnych zobowiązani są do zgłoszenia do IOD zapotrzebowania na szkolenie nowych pracowników oraz pracowników, którzy szkolenia z ochrony Danych Osobowych nie odbyli lub winni ponownie takie szkolnie odbyć.

ROZDZIAŁ VII
Nadawanie, zmiana lub usuwanie uprawnień w Systemach Informatycznych

1. Zarządzanie uprawnieniami Użytkowników Systemów Informatycznych, które nie należą do Centralnego Systemu Zarządzania Bezpieczeństwem Informacji odbywa się według poniższych zasad:
    1) W Systemie Informatycznym służącym do przetwarzania Danych Osobowych stosuje się system uwierzytelnienia.
    2) Każda osoba dopuszczona do przetwarzania Danych Osobowych posiada stosowne konto Użytkownika Systemu Informatycznego z odpowiednimi uprawnieniami.
    3) Przy tworzeniu nowego konta Użytkownika Systemu Informatycznego w systemie, Administrator Danych nadaje mu unikalny Identyfikator konta, który nie może być powtórzony dla żadnego innego Użytkownika Systemu Informatycznego przez cały okres zatrudnienia pracownika.
    4) Identyfikator umożliwia wykonywanie czynności zgodnie z zakresem powierzonych obowiązków, które wyznaczają poziom uprawnień.
    5) Procedurę nadawania uprawnień do przetwarzania Danych Osobowych w systemach należy stosować odpowiednio w przypadku zmiany uprawnień w Systemach Informatycznych lub w przypadku odebrania uprawnień w systemach, (**załącznik nr 6**)
    6) Zmiany dotyczące Użytkownika Systemu Informatycznego, takie jak rozwiązanie umowy o pracę lub umowy cywilno-prawnej, są przesłanką do natychmiastowego wyrejestrowania Użytkownika Systemu Informatycznego z Systemu Informatycznego oraz unieważnienie hasła i odnotowywanie tego faktu w ewidencji osób upoważnionych do przetwarzania Danych Osobowych.
    7) Prawa dostępu przyznane Użytkownikom Systemu Informatycznego, którzy nie są pracownikami etatowymi, powinny mieć okres czasowy i mogą być przyznawane wyłącznie na okres odpowiadający wykonywanemu zadaniu oraz powinny być formalnie zatwierdzane.
    8) Po przekroczeniu maksymalnej ilości prób uwierzytelnienia w systemie, konto powinno zostać zablokowane z możliwością jego odblokowania:
        a) Przez Administratora Danych.
        b) lub po 5 min konto odblokowuje się automatycznie.

2. Zarządzanie kontami Użytkowników Systemu Informatycznego:
    1) Konto Użytkownika Systemu Informatycznego winno zawierać odpowiedni Identyfikator, zabezpieczone hasłem tymczasowym, którego zmiana jest wymuszona przy pierwszym zalogowaniu Użytkownika Systemu informatycznego.
    2) Niedopuszczalne jest korzystanie z tego samego Identyfikatora przez więcej niż jednego Użytkownika Systemu Informatycznego.
    3) Identyfikator Użytkownika Systemu Informatycznego jest wpisywany do ewidencji osób upoważnionych do przetwarzania Danych Osobowych w Systemie Informatycznym wraz z zakresem upoważnienia oraz datą nadania uprawnień.
    4) Hasło uprawniające do korzystania z Aplikacji Użytkownika Systemu Informatycznego użytkownik wpisuje osobiście.
    5) Prawa dostępu nadawane w Systemie Informatycznym determinowane są rzeczywistymi obowiązkami służbowymi pracownika.
    6) Zmiana haseł Użytkownika Systemu Informatycznego w systemie jest wymuszana co 30 dni.
    7) Hasła składają się co najmniej z 8 znaków, zawierają małe i duże litery oraz cyfry lub znaki specjalne.
    8) Hasło nie może być ujawnione nawet po utracie przez nie ważności.
    9) Zabrania się zapisywania haseł, a w szczególności przechowywania ich w miejscach, których mogą się z nimi zapoznać osoby postronne.
3. Hasła w Systemach Informatycznych:
    1) Hasła nie mogą zawierać imion, nazwisk, przezwisk , inicjałów i innych kombinacji znaków mogących doprowadzić do łatwego rozszyfrowania haseł przez osoby nieupoważnione.
    2) Hasło początkowe, które jest przydzielone przez Administratora Systemu powinno umożliwiać Użytkownikowi Systemu Informatycznego zarejestrowanie się w systemie tylko jeden raz i powinno być natychmiast zmienione przez Użytkownika Systemu Informatycznego.
    3) Wszelkie urządzenia sprzętowe lub programowe, które na początku posiadały hasło domyślne, powinny mieć zmienione Hasło zgodnie z przyjętymi wymogami dotyczącymi formułowania Haseł.
    4) Należy unikać ponownego lub cyklicznego używania Haseł, które kiedyś były wykorzystywane.
    5) Hasła w stosunku, do których zaistniało podejrzenie o ich ujawnieniu, podlegają niezwłocznej zmianie.

ROZDZIAŁ VIII
Rozpoczęcie, zawieszenie i zakończenie pracy w systemie

1. Przed przystąpieniem do pracy z Systemem Informatycznym, Użytkownika Systemu Informatycznego zobowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony Danych Osobowych.
2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony Danych Osobowych, Użytkownika Systemu Informatycznego zobowiązany jest powiadomić o tym fakcie Administratora Danych i postępować zgodnie z zasadami określonymi w Polityce bezpieczeństwa.
3. Ustawienie monitora uniemożliwia wgląd w jego zawartość osobom nieuprawnionym.
4. Przy komputerze osoba trzecia może przebywać jedynie w obecności osoby uprawnionej.
5. Procedura rozpoczęcia pracy w systemie:
    1) Rozpoczynając pracę na komputerze Użytkownik Systemu Informatycznego z Artimed NZOZ Sp. z o.o. podaje Identyfikator i Hasło do systemu. Uruchamia Aplikację.
    2) Rozpoczyna pracę.

6. Procedura zawieszenia pracy w systemie:
    1) Przed opuszczeniem stanowiska należy upewnić się, czy na ekranie są otwarte dokumenty zawierające Dane Osobowe.
    2) W przypadku opuszczenia stanowiska pracy Użytkownika Systemu Informatycznego obowiązany jest zablokować stację roboczą bądź przymknąć ekran komputera przenośnego.
    3) Przed opuszczaniem miejsca pracy na dłuższy czas Użytkownika Systemu Informatycznego obowiązany jest:
        a) Poczekać, aż uaktywni się wygaszacz ekranu zabezpieczony hasłem, lub
        b) zablokować stację roboczą, lub
        c) wylogować się z systemu.
7. Procedura zakończenia pracy w systemie:
    1) Po zakończeniu pracy przy przetwarzaniu Danych Osobowych Użytkownika Systemu Informatycznego powinien prawidłowo wylogować się z systemu.
    2) Wyłączyć komputer.
    3) Zabezpieczyć stanowisko przed dostępem osób nieuprawnionych.

ROZDZIAŁ IX
Funkcjonalność Systemów Informatycznych za pomocą, których przetwarzane są Dane Osobowe przez Administratora Danych

1. Systemy Informatyczne, w których przetwarzane są Dane Osobowe zapewniają odnotowanie:
    1) Daty pierwszego wprowadzenia Danych Osobowych.
    2) Identyfikatora Użytkownika wprowadzającego dane.
    3) Informacji o odbiorcach, którym Dane Osobowe zostały udostępnione, dacie, zakresie tego udostępnienia i zapewnienie możliwości tego faktu w systemie zewnętrznym.
    4) Sprzeciwu wobec przetwarzania danych w celach marketingowych i zapewnienie możliwości tego faktu w systemie zewnętrznym.
2. Informacje o dacie pierwszego wprowadzenia i modyfikacji Danych Osobowych oraz identyfikatorze Użytkownika wprowadzającego i modyfikującego dane odnotowywane są w systemach wykorzystywanych do przetwarzania Danych Osobowych automatycznie, po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. Dla każdej osoby, której Dane Osobowe są przetwarzane w Systemie Informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje o: dacie pierwszego wprowadzenia Danych Osobowych, identyfikatorze Użytkownika wprowadzającego dane, udostępnieniach danych oraz o sprzeciwie wobec przetwarzania danych w celach marketingowych.
4. Dla krytycznych procesów biznesowych sieć komputerowa powinna być podłączona do zasilania zapasowego (zasilanie dwustronne, agregat prądotwórczy lub UPS). Oprogramowanie powinno zapewniać bezpieczne wyłączanie Systemu Informatycznego, po dokonaniu operacji zamknięcia w pracujących aplikacjach i oprogramowaniu systemowym.
5. Infrastruktura serwerowa powinna być zasilana przez UPS o parametrach, pozwalających na podtrzymanie napięcia przez czas pozwalający na wykonanie bezpiecznego wyłączenia serwera, tak by w związku z zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na zbiorach Danych Osobowych.

ROZDZIAŁ X
Kopie zapasowe, nośniki i ich przechowywanie

1. Szczegółowe instrukcje dotyczące tworzenia kopii zapasowych oraz sposobu ich przechowywania zostały zawarte w procedurze Tworzenia kopii zapasowych, **załącznik nr 5**

ROZDZIAŁ XI
Zasady monitorowania, przeglądu i konserwacji systemu

1. Za prawidłowość przeprowadzenia przeglądów, zapewnienia jakości, konserwację i dokumentowanie zmian w systemach odpowiadają wyznaczone osoby.
2. Przeglądy, naprawy i konserwacje Systemu Informatycznego, które będą przeprowadzane w miejscu użytkowania tego systemu, wykonywane są pod nadzorem Administratora Systemu Informatycznego lub innej wyznaczonej osoby.
3. W przypadku, gdy konieczne jest dokonanie przeglądu, naprawy lub konserwacji Systemu Informatycznego poza miejscem jego użytkowania, z urządzenia należy wymontować element, na którym zapisane są Dane Osobowe, o ile jest to możliwe. W przeciwnym wypadku należy zawrzeć z podmiotem dokonującym naprawy umowę powierzenia.
4. Prace dotyczące przeglądów, konserwacji i napraw wymagające zaangażowania autoryzowanych firm zewnętrznych, są wykonywane przez uprawnionych przedstawicieli tych firm (serwisantów) pod nadzorem Administratora Systemu Informatycznego lub innej wyznaczonej osoby. Przy stałych czynnościach serwisowych należy zawrzeć umowę powierzenia przetwarzania danych, dla czynności jednorazowych serwisant podpisuje oświadczenie o poufności zgodnie ze wzorem **załącznik nr 2**
5. Przegląd programów i narzędzi programowych powinien być przeprowadzany w przypadku zmiany wersji oprogramowania Aplikacji, zmiany wersji oprogramowania bazy danych lub wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.
6. Aplikacje muszą być zgodne z Polityką bezpieczeństwa Spółki Artimed NZOZ.

ROZDZIAŁ XII
Upoważnienie do przetwarzania Danych Osobowych

1. Do przetwarzania Danych Osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych.
2. Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania Danych Osobowych.
3. Administrator Danych wydaje osobom przetwarzającym Dane Osobowe upoważnienie sporządzane wg wzoru stanowiącego **załącznik nr 1** do niniejszej Polityki.
4. Upoważnienie do przetwarzania Danych Osobowych obowiązuje do czasu ustania stosunku pracy lub obowiązków związanych z przetwarzaniem Danych Osobowych.
5. Upoważnienia, o których mowa powyżej, są przechowywane w aktach osobowych pracownika.
6. Osoby upoważnione są wpisane przez osobę odpowiedzialną za sprawy personalne lub inną osobę wyznaczoną przez Prezesa do rejestru „Ewidencja osób upoważnionych do przetwarzania Danych Osobowych", której wzór stanowi **załącznik nr 3** do niniejszej Polityki Bezpieczeństwa.

ROZDZIAŁ XIII
Obszary przetwarzania Danych Osobowych

1. Dane Osobowe mogą być przetwarzane w obszarach przetwarzania Danych Osobowych, na które składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie Administrator Danych prowadzi działalność. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących „Wykaz obszarów przetwarzania Danych Osobowych", w którym te Dane Osobowe są przetwarzane stanowi **załącznik nr 4**.
2. Przebywanie osób nieuprawnionych w pomieszczeniach, w których przetwarzane są Dane Osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą Administratora Danych.
3. Pomieszczenia, w których przetwarzane są Dane Osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania Danych Osobowych, w sposób ograniczający możliwość dostępu do nich osobom nieupoważnionym.

4. Osoby upoważnione zobowiązane są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są Dane Osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w miejscu powszechnie dostępnym (np. w zamku drzwi).
5. Obszarami przetwarzania Danych Osobowych są również te miejsca, w których składowane są dokumenty z Danymi Osobowymi na mocy zawartych umów z innymi podmiotami (np. archiwa zewnętrzne).

ROZDZIAŁ XIV
Wykaz czynności przetwarzania Danych Osobowych

1. Prowadzony jest w Rejestrze czynności przetwarzania Danych Osobowych.

ROZDZIAŁ XV
Opis struktury zbiorów Danych Osobowych

1. Podstawowymi programami wykorzystywanymi do przetwarzania Danych Osobowych u Administratora Danych są specjalizowane aplikacje oraz pakiet biurowy Office.
2. Zawartość pól informacyjnych występujących w systemach zastosowanych musi być zgodna z celem przetwarzania Danych Osobowych.
3. Opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązań między nimi jest prowadzony przez Artimed NZOZ Sp. z o.o., **załącznik nr 7**

ROZDZIAŁ XVI
Powierzanie przetwarzania Danych Osobowych

1. Zasady dotyczące powierzenia przetwarzania Danych Osobowych zostały zawarte w procedurze Powierzenia przetwarzania Danych Osobowych

ROZDZIAŁ XVII
Udostępnianie i Przekazywanie Danych Osobowych

1. Dane Osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.
2. Udostępniając Dane Osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
3. Dokumenty papierowe muszą być przekazywane lub przesyłane w sposób uniemożliwiający utratę ich poufności i integralności.
4. Korespondencja powinna być dostarczana przez uprawnionych operatorów. Niezależnie od tego korespondencję może dostarczać również upoważniony Pracownik Spółki Artimed NZOZ.

ROZDZIAŁ XVIII
Sposób przepływu danych pomiędzy poszczególnymi systemami

1. Dokumentacja zawierająca sposób przepływu danych pomiędzy systemami, jest prowadzona przez Artimed NZOZ Sp. z o.o., a nadzór nad jej poprawnością i integralnością sprawuje ASI.

ROZDZIAŁ XIX
Naruszenie bezpieczeństwa przetwarzania Danych Osobowych

1. Proces zgłaszania naruszeń bezpieczeństwa przetwarzania Danych Osobowych został opisany w procedurze Zgłaszania naruszeń ochrony Danych Osobowych.

ROZDZIAŁ XX
Postanowienia końcowe

2. Kierownicy jednostek organizacyjnych zobowiązani są poinformować podległych pracowników o regulacji wynikającej z niniejszego aktu organizacyjnego oraz zobowiązani są wyegzekwować stosowanie się do postanowień w nim zawartych przez wszystkich pracowników Spółki.

Administrator Danych

ZAŁĄCZNIKI:

Załącznik nr 1 – Wzór upoważnienia do przetwarzania Danych Osobowych.
Załącznik nr 2 – Wzór oświadczenie o obowiązku zachowaniu zasad poufności dla pracowników
Załącznik nr 3 – Wzór ewidencja osób upoważnionych do przetwarzania Danych Osobowych
Załącznik nr 4 – Wykaz obszarów przetwarzania Danych Osobowych
Załącznik nr 5 – Procedura tworzenia kopii zapasowych
Załącznik nr 6 – Wniosek o nadanie uprawnień w systemie informatycznym
Załącznik nr 7 – Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

(imię i nazwisko)

(stanowisko)

Upoważnienia do przetwarzania Danych Osobowych

Na podstawie przyjętej w Artimed NZOZ Sp. z o.o. Polityki bezpieczeństwa (upoważniam Panią/Pana* zatrudnioną/ego* w Artimed NZOZ Sp. z o.o. z siedzibą w Kielcach, ul Paderewskiego 4B do przetwarzania danych osobowych w związku z wykonywaną pracą wynikającą z działań przeprowadzanych na Danych Osobowych.

Upoważnienie obejmuje* prawo wglądu, wprowadzenia, modyfikacji i usuwania Danych Osobowych w zakresie niezbędnym do realizacji swych zadań służbowych.

……..
(podpis i pieczęć Administratora Danych)

*niepotrzebne skreślić

……
Miejscowość, data

Oświadczenie o obowiązku zachowaniu zasad poufności dla pracowników

Ja, niżej podpisany /-a

……
(Imię i Nazwisko)

PESEL……

Zobowiązuję się do zachowania w tajemnicy wszelkich informacji, z którymi zapoznałam/-em się w trakcie wykonywania mojej pracy, a w szczególności zobowiązuję się do nieprzekazywania żadnych informacji dotyczących stanu zdrowia pacjentów, w jakiejkolwiek formie, jakiejkolwiek osobie trzeciej w trakcie trwania umowy, jak i po jej rozwiązaniu.

Zobowiązuję się do przestrzegania zobowiązań zawartych w niniejszym oświadczeniu w okresie obowiązywania stosunku pracy (lub innego stosunku prawnego) oraz po ustaniu mojego zatrudnienia.

Oświadczam, że zapoznałam/em się z przepisami dotyczącymi ochrony Danych Osobowych, a także z regulacjami wewnętrznymi dotyczącymi ochrony informacji w Artimed NZOZ Sp. z o.o.

Oświadczam, że znana jest mi odpowiedzialność karna wynikająca z niżej wymienionych aktów prawnych:

1. Ustawa z dnia 26 czerwca 1974r. Kodeks pracy (Dz.U. 2014r. poz. 1502 z późn. zm.),
2. Ustawa z dnia 6 czerwca 1997r. Kodeks karny (Dz.U. 1997r. Nr 88, poz. 553 z późn. zm.),
3. Ustawa z dnia 16 kwietnia 1993r. o zwalczaniu nieuczciwej konkurencji (Dz.U. nr 153, poz. 1503 z późn. zm.),
4. Ustawa z dnia 6 listopada 2008r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. 2012r poz. 159 z późn. zm.),
5. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
6. Ustawy o ochronione danych osobowych.

…… ……
Podpis osoby przyjmującej oświadczenie *Podpis pracownika*

Ewidencja osób upoważnionych do przetwarzania Danych Osobowych w Artimed NZOZ Sp. z o.o.

Lp.	Imię i nazwisko Użytkownika	Identyfikator Użytkownika w domenie	Data nadania upoważnienia (RRRR/MM/DD)	Data odebrania upoważnienia (RRR/MM/DD)

Wykaz obszarów przetwarzania Danych Osobowych

MIASTO	ADRES
25-017 KIELCE	Ul. Paderewskiego 4B
25-709 KIELCE	Ul. Mielczarskiego 93-95
25-328 KIELCE	Ul. Śląska 13

WYKAZ POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Lp.	Nazwa zbioru danych (1)	Lokalizacja	Rodzaj kondygnacji/ numery pomieszczeń (2)	Zastosowane zabezpieczenia fizyczne (3)
1	Pacjenci	Siedziba Artimed NZOZ Sp. z o.o. 25-017 Kielce ul. Paderewskiego 4B	PARTER I PIĘTRO II PIĘTRO III PIĘTRO IV PIĘTRO V PIĘTRO	(POMIESZCZENIE T23- S, K, Z, U, A, ZA, ZP, SK, W, KL) (POZOSTAŁE POMIESZCZENIA – U, ZA, KL)
		Oddział Artimed NZOZ Sp. z o.o. 25-328 Kielce, ul. Śląska 13	PARTER	U, ZA, KL
		Oddział Artimed NZOZ Sp. z o.o. 25-709 Kielce, ul. Mielczarskiego 93-95	PARTER	U, ZA, KL, KR
2	Zbiór Kadrowo-Płacowy (umowy o pracę z pracownikami, umowy cywilno-prawne, byli pracownicy,	Siedziba Artimed NZOZ Sp. z o.o. 25-017 Kielce ul. Paderewskiego 4B	VI PIĘTRO klatka A	U, K, SK, KD, ZA, KL

	kandydaci do pracy)			
3	Zbiór Udziałowców Artimed NZOZ Sp. z o.o.	Siedziba Artimed NZOZ Sp. z o.o. 25-017 Kielce ul. Paderewskiego 4B	VI PIĘTRO klatka A	U

Legenda:

(1) - Wydzielona fizycznie sieć

(2) - (S) – serwer, (K) – miejsce przechowywania kopii bezpieczeństwa, (Z) – pomieszczenie w którym wykonywane są kopie bezpieczeństwa, (U) – pomieszczenie osób przetwarzających dane zamykane na klucz, (A) – pomieszczenie administratora systemów informatycznych

(3) - (W) – wzmocnienie drzwi, (KD) – kontrola dostępu, (CTV) – dozór kamery przemysłowej, (SA) – system antywłamaniowy, (CZ) – czujka zbicia szyby, (CZW) – czujka zalania wodą, (ZA) – zasilanie awaryjne z UPS, (AP) – zasilanie awaryjne z agregatu prądotwórczego, (KL) – klimatyzacja, (SP) – dodatkowa sygnalizacja PPOŻ, (ZP) – zamki patentowe, (KR) – krata antywłamaniowa w oknie, (SF)- Sejf, (SK)- szafa zamykana na klucz

PROCEDURA TOWRZENIA KOPII ZAPASOWYCH

1. Zbiory Danych Osobowych oraz programy i narzędzia programowe służące do ich przetwarzania, zapisywane na nośnikach zewnętrznych (np. streamer, dyski: wymienne, magnetyczne, optyczne) tworzące kopie zapasowe kolejnych okresów, służące do odtwarzania oryginalnych danych w przypadku ich utraty lub uszkodzenia.
2. Kopie z pkt.1 powinny być:
    1) Zapisywane na nośnikach magnetycznych lub magnetooptycznych, które cechują się odpowiednią trwałością.
    2) Zapisywane docelowo do dwóch różnych lokalizacji.
    3) Sporządzane regularnie na zasadach określanych wewnętrzną procedurą przez wewnętrzny dział IT Spółki Artimed NZOZ. Dział IT odpowiada za przechowywanie oraz sprawdzanie poprawności wykonania kopii zapasowych na nośnikach.
3. Nośniki z pkt. 2 powinny być:
    1) Unikalnie oznakowane w danym systemie tworzenia/odtwarzania kopii zapasowych oraz przechowywane w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach odrębnych od pomieszczeń, w których przetwarzane są zbiory danych w trybie bieżącym.
    2) Przechowywane w odpowiednich warunkach środowiskowych w szafach lub sejfach przystosowanych do przechowywania nośników danych.
    3) Ewidencjonowane od momentu zapisania na nich danych do momentu ich utylizacji.
    4) W przypadku gdy zawierają dane medyczne konieczne ich szyfrowanie.
4. Pomieszczenia z pkt. 3 powinny znajdować się poza budynkiem, gdzie przetwarzane są zbiory danych oraz ich kopie zapasowe.
5. Kopie zapasowe, które uległy uszkodzeniu lub ustała ich użyteczność podlegają natychmiastowemu zniszczeniu z zachowaniem procedur określonych w niniejszej procedurze:
    1) Niszczenie nośników magnetycznych i optycznych, na których zapisane są kopie zapasowe odbywa się zgodnie z umową utylizacyjną obowiązującą w Artimed NZOZ Sp. z o.o. w obecności pracownika IT z wyłączeniem nośników utworzonych i wykorzystywanych przez pracownika bez wiedzy IT.
    2) Z nośników magnetycznych i optycznych wielokrotnego użytku, np. CDRW, dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku, gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym odzyskanie danych.
    3) Dane zawarte na nośnikach optycznych jednokrotnego użytku, np. CDR, należy usuwać poprzez całkowite zniszczenie nośnika.

Przechowywanie Nośników zawierających Dane Osobowe

1. Dane Osobowe mogą być przechowywane:
    1) Na serwerach zlokalizowanych w obszarach wyznaczonych do przetwarzania Danych Osobowych.
    2) Na stacjach roboczych.
    3) Na wymiennych Nośnikach elektronicznych.
2. Wymienne Nośniki elektroniczne, o ile nie są użytkowane, powinny być przechowywane w zamykanych szafkach.
3. Wszystkie informacje zawierające Dane Osobowe przechowywane w formie elektronicznej na nośnikach podlegają szczególnej ochronie.
4. Nośniki magnetyczne i optyczne z danymi osobowymi przechowywane będą przez okres nie dłuższy niż czas wykorzystania lub możliwego wykorzystania danych na nich zapisanych, w zabezpieczonych pomieszczeniach.

5. Nośniki zawierające Dane Osobowe przechowywane są w miejscach uniemożliwiających dostęp do nich osobom nieupoważnionym.
6. Jeżeli dysk twardy jest uszkodzony i nie ma możliwości usunięcia z niego Danych Osobowych, należy wymontować go z komputera i zniszczyć. Dostawca usługi dla Spółki Artimed NZOZ jest odpowiedzialny za utylizację dysków zgodnie z wewnętrznymi regulacjami, określone w procedurze „Usunięcie danych/trwałe zniszczenie nośnika danych".
7. Likwidacji zniszczonych lub niepotrzebnych Nośników magnetycznych lub optycznych dokonuje się w sposób uniemożliwiający odczytanie zamieszczonych na nich danych, zgodnie z umową utylizacyjną w obecności pracownika IT.
8. Urządzenia, dyski lub inne Nośniki informacji zawierające Dane Osobowe nie nadające się do naprawy należy zniszczyć w sposób uniemożliwiający odczytanie zapisanych na nich informacji zgodnie z umową utylizacyjną w obecności pracownika IT.
9. Dane są składowane na nośnikach taśmowych lub innych zapewniających podobną trwałość.
10. Zalecane jest przepisywanie starych technologii na nowe.
11. Standard w Polityce utrzymywania kopii zapasowych dla poszczególnych obiektów:
    1) FILESYSTEMY – kopie zapasowe wykonywane w trybie „cold backup" o standardowej retencji 30 dni
        a) Kopie pełne tygodniowe.
        b) Kopie przyrostowe oraz różnicowe codziennie prócz dni, w które wykonują się kopie pełne.
    2) BAZA DANYCH – kopie zapasowe wykonywane w trybie „hot backup" o standardowej retencji 30 dni
        a) Kopie pełne i tygodniowe.
        b) Kopie przyrostowe oraz różnicowe codziennie prócz dni, w które wykonują się kopie pełne.
    3) SYSTEMY OPERACYJNE dla maszyn fizycznych – kopie zapasowe wykonywane narzędziem natywnym dla danego systemu operacyjnego i przekazywane do systemu backupu o standardowej retencji 30 dni
    4) SYSTEMY OPERACYJNE dla maszyn wirtualnych – kopie zapasowe wykonywane w trybie „crash consitetnt" o standardowej retencji 30 dni
        a) Kopie pełne tygodniowe.
        b) Kopie przyrostowe, codziennie prócz dni, w które wykonują się kopie pełne.

WNIOSEK
O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

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

Imię i nazwisko użytkownika:	**Wydział/biuro/samodzielne stanowisko**
Opis i zakres uprawnień użytkownika w systemie informatycznym	
Data wystawienia:	Podpis bezpośredniego przełożonego użytkownika systemu:
Podpis Administratora Systemu:	Akceptacja ABI

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Lp.	Nazwa zbioru danych osobowych	Forma danych (1)	Zastosowane oprogramowanie	Zabezpieczenia informatyczne (2)	Zarządzający zbiorem
1	Pacjenci NZOZ	E, P	KS-SOMED (moduły: Gabinet, Terminarz, Zlecenia, Rozliczenia, Umowy, Zestawienia, Kasa, Kartoteki) INSERT GT, WINDOWS 10, WINDOWS 7, MS OFFICE	D, S, AD, DLP	
2	Zbiór Kadrowo-Płacowy (umowy o pracę z pracownikami Artimed, umowy cywilno-prawne, dokumentacja byłych pracowników, dokumentacja kandydatów do pracy	E, P	PŁATNIK wersja 10, WINDOWS 7, MS OFFICE	D, S, AD, DLP	Dyrektor Finansowy Główny Księgowy
3	Zbiór Udziałowców Artimed NZOZ Sp. z o.o.	E, P	System Bankowości Internetowej, WINDOWS 7, MS OFFICE	D, S, AD, DLP	Dyrektor Finansowy Główny Księgowy

LEGENDA

(1) - np.: (E) dokumenty elektroniczne, (P) dokumenty papierowe

(2) - np.; (D) dwustopniowa autoryzacja - indywidualne hasło dostępu: do domeny oraz do aplikacji, (S) szyfrowanie transmisji danych SSL VPN, (F) wydzielona fizycznie sieć, (DLP) zastosowany system bezpiecznego przetwarzania danych, (AD) funkcja Active Directory