Wojewódzki Specjalistyczny Zespół
Zakładów Opieki Zdrowotnej
Chorób Płuc i Gruźlicy
w Wolicy k/Kalisza

Wojewódzki Specjalistyczny Zespół Zakładów Opieki Zdrowotnej Chorób Płuc i Gruźlicy w Wolicy k/ Kalisza

Polityka Zarządzania Systemem Teleinformatycznym

	Stanowisko:	Imię i nazwisko:	Data:	Podpis:
Opracował	Administrator Systemu Informatycznego	Robert Krymarys	15.06.2021 r.	
Zatwierdził pod względem merytorycznym:	Inspektor Ochrony Danych Osobowych	Jacek Gołdych	15.06.2021 r.	INSPEKTOR Ochrony Danych Osobowych Jacek Gołdych
Zatwierdził pod względem formalno – prawnym	Dyrektor WSZZOZ	Sławomir Wysocki	15.06.2021 r.	DYREKTOR Wojewódzkiego Specjalistycznego ZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza lek. med. Sławomir Wysocki

ROZDZIAŁ I.

POSTANOWIENIA OGÓLNE

1.1. Polityka Zarządzania Systemem Teleinformatycznym, zwana dalej **„Polityką ZST"**, określa zasady i tryb postępowania Wojewódzkim Specjalistycznym Zespole Zakładów Opieki Zdrowotnej Chorób Płuc i Gruźlicy w Wolicy oraz Wojewódzkiej Przychodni Chorób Płuc i Gruźlicy w Kaliszu, ul. Majkowska 13 A i innych zakładów opieki zdrowotnej działających w ramach zespołu, (dalej łącznie SZPITAL) i osób przez nią upoważnionych przy przetwarzaniu danych osobowych w systemach informatycznych.

1.2. Polityka ZST została opracowana w oparciu o § 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024) i została zaktualizowana i dostosowana do wymogów Ogólnego Rozporządzenia 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 (ogólne rozporządzenie o ochronie danych - RODO) i stanowi integralną część **Polityk Danych Osobowych** w ramach dokumentacji bezpieczeństwa danych osobowych.

1.3. Polityka Zarządzania Systemem Teleinformatycznym ma na celu zapewnienie właściwego zarządzania systemem IT oraz ochronę zgromadzonych w nim danych, jak również jednolite i bezpieczne warunki korzystania z danych gromadzonych w zbiorach danych osobowych, zarówno tych, których Szpital jest samodzielnym Administratorem, jak i tych, które zostały powierzone Szpitalowi przez Kontrahentów do przetwarzania w zakresie i celu przewidzianym w umowie, a których Szpital jest Procesorem.

1.4. Podstawowym celem zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych w zbiorach danych osobowych Szpitala jest zapewnienie jak najwyższego standardu bezpieczeństwa tych danych. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania, charakteru poufnego wraz z zachowaniem ich poufności, integralności, rozliczalności i dostępności oraz integralności systemu informatycznego służącego do przetwarzania danych.

1.5. W celu zwiększenia efektywności ochrony danych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku stopni ochronnych.

1.6. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:

a. rozliczalność danych - dostęp do danych tylko i wyłącznie osobom uprawnionym na każdym etapie ich przetwarzania,

b. integralność danych - niezmienialność danych w sposób nieuprawniony,

c. poufność danych - dostęp do danych tylko i wyłącznie osobom uprawnionym, a wyeliminować ujawnienie i dostęp do nich osobom nieuprawnionym,

d. ochrona przed zniszczeniem danych w sposób nieuprawniony,

e. dostępność danych,

f. integralność systemu /rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej/.

1.7. Realizację zamierzeń określonych wyżej powinna zagwarantować następująca strategia:

a. wdrożenie procedur określających postępowanie osób zatrudnionych przy przetwarzaniu danych osobowych,

b. przeszkolenie użytkowników w zakresie ochrony danych osobowych oraz zaznajomienie z przepisami dotyczącymi ochrony danych osobowych,

c. przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację /hasła, identyfikatory/,

d. korzystanie z oprogramowania systemowego i użytkowego spełniającego odpowiednie standardy,

e. zaimplementowanie w systemie informatycznym zabezpieczeń zapewniających nienaruszoną pracę systemu, w tym najnowszych wersji oprogramowania antywirusowego,

f. ocena ewentualnych zagrożeń bezpieczeństwa systemu informatycznego i ryzyk związanych z jego obsługą,

g. wdrożenie zabezpieczeń o charakterze fizycznym pomieszczeń, korytarzy, budynku, stosownie do zagrożeń i ryzyk wynikających z oceny, o której mowa w pkt. 6,

h. stałe monitorowanie wdrożonych zabezpieczeń w celu identyfikacji podatnych na zagrożenia obszarów i słabości zabezpieczeń,

i. podejmowanie niezbędnych działań dla likwidacji słabych ogniw w systemie zabezpieczeń,

j. okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych.

1.8. Polityka Ochrony Danych Osobowych określająca zadania, które należy realizować dla zapewnienia spójności wszystkich zabezpieczeń systemu, została sformułowana w odrębnym dokumencie i odzwierciedla podstawowe zasady bezpieczeństwa danych osobowych w Szpitalu.

1.9. Terminologia:

SYSTEM INFORMATYCZNY	Elektroniczny system przetwarzania informacji Szpitala wraz zasobami technicznymi, który dostarcza i rozprowadza informacje,
ZBIÓR DANYCH	każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
USUWANIE DANYCH	rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą, w tym pseudonimizacji i anonimizację
PRZETWARZANIE DANYCH	rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
DANE OSOBOWE	uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych

	czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
BAZA DANYCH	zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych danych. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane.
ADMINISTRATOR	rozumie się przez to w zależności od zbioru danych osobowych: a) osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, który na podstawie art. 28 – Ogólnego Rozporządzenia 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), powierzył do Szpitala przetwarzanie danych w drodze umowy zawartej na piśmie, w zakresie i celu przewidzianym w umowie; b) **Wojewódzki Specjalistyczny Zespół Zakładów Opieki Zdrowotnej Chorób Płuc i Gruźlicy w Wolicy** oraz **Wojewódzka Przychodnia Chorób Płuc i Gruźlicy w Kaliszu, ul. Majkowska 13 A i inne zakłady opieki zdrowotnej działających w ramach zespołu,** (dalej łącznie **SZPITAL)**
PROCESOR / PRZETWARZAJĄCY DANE	Szpital – w przypadku danych powierzonych przez zewnętrznych administratorów w systemie informatycznym Szpitala
INSPEKTOR OCHRONY DANYCH	powołana przez Podmiot osoba odpowiedzialna za bezpieczeństwo danych osobowych, upoważniona wraz z Administratorem Systemu Informatycznego do ustalania identyfikatorów i pierwszych haseł dostępu użytkowników do aplikacji, które obsługują oraz do nadzoru i kontroli w zakresie określonym przepisami o ochronie danych osobowych oraz regulacjami wewnętrznymi Szpitala,
ADMINISTRATOR SYSTEMU INFORMATYCZNEGO /KIEROWNIK DZIAŁU KONTROLINGU I IT	- osoba odpowiedzialna za system informatyczny i upoważniona wraz z Inspektorem Ochrony Danych do ustalania identyfikatorów i pierwszych haseł dostępu użytkowników do aplikacji, które obsługują oraz do nadzoru i kontroli w zakresie określonym m.in. przepisami o ochronie danych osobowych oraz regulacjami wewnętrznymi Szpitala, oraz odpowiedzialna za prawidłowe funkcjonowanie powierzonego jej do administrowania systemu informatycznego, określenie to obejmuje zarówno

	administratorów systemów operacyjnych jak i aplikacji użytkowych, - każda inna osoba działająca w ramach struktury działu IT Szpitala pełniąca rolę administratora systemu informatycznego w ramach obowiązków służbowych/pracowniczych lub umownych w ramach umowy cywilnej (np. dzieło/zlecenie)
UŻYTKOWNICY	osoby wyznaczone przez Szpital upoważnione do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, które posiadają ustalony identyfikator oraz hasło, uprawnione do dostępu do danych osobowych gromadzonych w kartotece ewidencyjnej,
PRACOWNIK OCHRONY	osoba wykonująca zadania ochrony na rzecz Szpitala
JEDNOSTKA ORGANIZACYJNA	Samodzielna jednostka organizacyjna podporządkowana administracyjnie Wojewódzkiemu Specjalistycznemu Zespołowi Zakładów Opieki Zdrowotnej Chorób Płuc i Gruźlicy w Wolicy w szczególności a) Wojewódzka Przychodnia Chorób Płuc i Gruźlicy w Kaliszu, ul. Majkowska 13 A b) i inne zakłady opieki zdrowotnej działających w ramach zespołu,
KOMÓRKA ORGANIZACYJNA	każda komórka wydzielona organizacyjnie i funkcjonalnie, zgodnie z Regulaminem organizacyjnym Przetwarzającego Dane.

ROZDZIAŁ II.

ZASADY OGÓLNE

1. Pracownicy lub współpracownicy Szpitala nie są uprawnieni do instalacji jakiegokolwiek prywatnego oprogramowania bez uprzedniej zgody Administratora. W przypadku zainstalowania takiego oprogramowania bez odpowiedniej akceptacji pracownik ponosi odpowiedzialność porządkową tytułem naruszenia postanowień niniejszej Polityki.
2. Oprogramowanie na komputerach firmowych może być zainstalowane wyłącznie przez Administratora Systemów Informatycznych lub upoważnione przez niego osoby.
3. Dane zapisane na komputerach firmowych związane z wykonywanymi obowiązkami służbowymi powinny być szczególnie chronione i stanowią informacje, których dysponentem jest Szpital.
4. Świadome użytkowanie udostępnionych zasobów w tym systemów komputerowych lub infrastruktury informatycznej przez użytkownika w sposób powodujący zakłócanie stabilności ich pracy jest niedozwolone. W szczególności niedozwolone jest pobieranie lub wysyłanie z/do sieci publicznej Internet danych w dużych ilościach. W przypadku wątpliwości co do właściwego użytkowania udostępnionych zasobów należy poradzić się Administratora Systemów Informatycznych.

b. hasło zawiera znaki co najmniej z 3 grup: małe litery, wielkie litery, cyfry, znaki specjalne (np. # %!, „).

c. Hasło użytkownika musi różnić się od jego 6 poprzednich haseł,

d. nie mogą być zapisywane w systemie w postaci jawnej,

e. co do zasady nie powinny być w nich używane imiona, nazwiska, przezwiska, inicjały, numery telefonów użytkownika, numery rejestracyjne pojazdów, nazwa firmy lub skrótu i inne kombinacje znaków mogących doprowadzić do łatwego rozszyfrowania haseł przez osoby nieupoważnione,

f. nie mogą być w nich stosowane znaki następujące po sobie na klawiaturze bądź kombinacje tych samych liter czy cyfr.

11. Hasła powinny być zmieniane co najmniej co 30 dni.

12. Hasła podlegają natychmiastowej zmianie w przypadku podejrzenia odkrycia ich przez nieupoważnioną osobę.

13. Elementy systemu informatycznego związane z bezpieczeństwem dostępu są tak sparametryzowane, aby wymusić stosowanie podanych zasad. Niezastosowanie tych zasad przez użytkownika powoduje odmowę dostępu do systemu.

14. Hasła nie mogą być nigdzie zapisywane, z wyjątkiem hasła dla Inspektora Ochrony Danych, które przechowywane jest w opieczętowanej kopercie, w miejscu wyznaczonym przez Administratora.

a. Tryb udostępniania hasła Inspektora Ochrony Danych określa Załącznik Nr 14 Polityki Ochrony Danych Osobowych.

b. Postanowienia paragrafów 8, 9 i 10 stosuje się odpowiednio.

15. Prawidłowe wykonywanie obowiązków związanych z korzystaniem użytkowników z haseł nadzoruje Inspektor Ochrony Danych lub Administrator. Nadzór ten w szczególności polega na monitorowaniu funkcjonowania mechanizmu uwierzytelniania i doprowadzeniu do przywrócenia stanu prawidłowego w przypadku nieprawidłowości.

16. Administrator Systemu Informatycznego w przypadku nieobecności pracownika w porozumieniu z Inspektorem Ochrony Danych Osobowych ma prawo uzyskać dostęp do plików użytkownika korzystając z konta administratora skonfigurowanego na każdym stanowisku.

C. Rejestrowanie i wyrejestrowywanie użytkowników

1. Ewidencję użytkowników prowadzi, w imieniu Podmiotu, Inspektor Ochrony Danych lub osoby przez niego upoważnione.

2. Ewidencja zawiera:

a. nazwisko i imię użytkownika,

b. wskazanie komórki organizacyjnej, w której jest zatrudniony,

c. identyfikator użytkownika.

3. Ewidencja użytkowników prowadzona jest w systemie komputerowym, wg wzoru określonego w załączniku nr 2 Polityki Ochrony Danych Osobowych.

4. Nośniki magnetyczne, na których gromadzone są wykazy zawierające ewidencję użytkowników przechowywane są w pomieszczeniach, do których ma dostęp tylko Inspektor Ochrony Danych lub osoby przez niego upoważnione.

5. Zmiany dotyczące użytkownika, takie jak:

a. zmiana służbowego adresu lub telefonu,

b. zmiana nazwiska,

c. zmiana identyfikatora,

podlegają niezwłocznemu odnotowaniu w ewidencji.

6. Zmiany dotyczące użytkownika, takie jak:

a. rozwiązanie umowy o pracę,

b. utrata upoważnienia,

c. zmiana zakresu obowiązków służbowych wiążąca się z utratą dostępu do danych powodują wyrejestrowanie użytkownika, w trybie natychmiastowym, z ewidencji, o której mowa ust. 2, pkt C, rozdziału II, unieważnienie jego identyfikatora z systemu informatycznego oraz unieważnienie hasła tego użytkownika.

7. Kierownicy komórek organizacyjnych Przetwarzającego Dane odpowiadają za natychmiastowe zgłaszanie użytkowników - do osób upoważnionych - którzy utracili uprawnienia do dostępu do odpowiednich aplikacji, celem zablokowania im dostępu do systemu informatycznego poprzez unieważnienie identyfikatora i wykreślenie z ewidencji użytkowników, o której mowa w ust. 1.

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

9. Inspektor Ochrony Danych obowiązany jest gromadzić identyfikatory, które utraciły ważność lub też stosować odpowiednie ich oznaczenie.

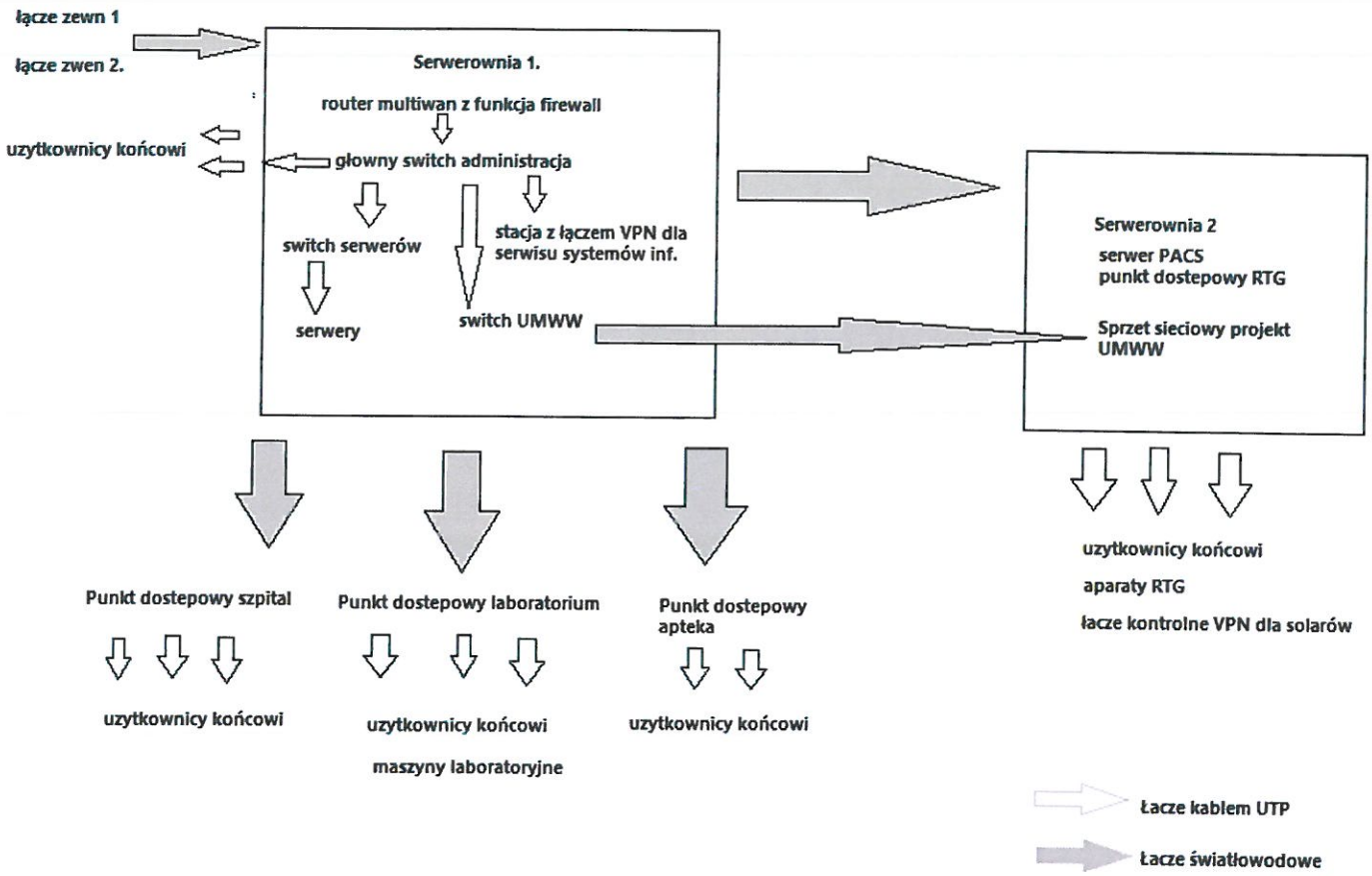
ROZDZIAŁ IV.

A. OGÓLNE INFORMACJE O SYSTEMIE INFORMATYCZNYM

W Szpitalu używanych jest kilka różnych systemów informatycznych. Wspólnie stanowią one jedno środowisko informatyczne, którym zarządza Administrator Systemu Informatycznego, zajmujący się poszczególnymi systemami oraz infrastrukturą w ramach swoich kompetencji. Środowisko informatyczne obsługuje i obejmuje swym działaniem Szpital.

B. Architektura systemu

System sieciowo komputerowy wykonany jest w standardzie ethernet, na zasadzie drzewa. Rdzeniowe połączenia zrealizowane są za pomocą sieci światłowodowej (łącze zewnętrzne oraz komunikacja pomiędzy poszczególnymi budynkami). Pozostałe łącza w ramach sieci oraz przyłącza do poszczególnych gniazd abonenckich zrealizowano za pomocą sieci Ethernet 1GB/s z pomocą kabla S/UTP min cat5e.



W Przychodni Chorób Płuc jest używana własna wewnętrzna sieć Ethernet i wi-fi. Łącze zewnętrzne to łącze 4g, sieć wewnętrzna obejmuje router z funkcja firewall, sieć wi-fi 5 GHz dostępną tylko na skonfigurowanych przez administratora urządzeniach oraz siec kablowa Ethernet (podłączenie bezpośrednio do routera).
Odziały zewnętrzne łączą się z infrastrukturą sieciową poprzez VPN, maja dostęp tylko do systemu teleinformatycznego. Z wyjątkiem Administratora Danych Osobowych bądź osób przez niego upoważnionych.

C. Łącza transmisji danych

Lokalizacje zewnętrzne poza sieć lokalną połączone są łączami stałymi symetrycznymi lub asymetrycznymi o przepustowości zależnej od potrzeb biura i dostępności łącza.
Urządzenia teletransmisji są chronione przed bezpośrednim fizycznym dostępem osób niepowołanych, a dostęp sieciowy (zdalny) zabezpieczony jest poprzez konieczność autoryzacji za pomocą identyfikatora i hasła. Użyto również odrębnych podsieci do odseparowania ruchu sieciowego dla niepowiązanych ze sobą użytkowników i systemów.

D. Oprogramowanie systemowe

Systemy operacyjne serwerów są z rodziny Microsoft Windows Server lub Linux. Jako System Bazy Danych wykorzystywany jest Microsoft SQL, Server Oracle oraz Microsoft Access. Konfiguracja systemu bazodanowego charakteryzuje się brakiem bezpośredniego dostępu użytkowników do baz danych oraz brakiem możliwości bezpośredniej modyfikacji danych w bazach danych. Dostęp użytkowników do baz danych jest możliwy tylko pośrednio poprzez zainstalowane systemy informatyczne na komputerach użytkowników.
Stacje robocze użytkowników pracują pod kontrolą systemów operacyjnych z rodziny Microsoft Windows.

W Szpitalu działa system pocztowy w oparciu o usługę hostingową z odpowiednim zabezpieczeniem antywirusowym i antyspamowym, za które odpowiedzialny jest usługodawca.

B. WYMAGANIA DOTYCZĄCE SPRZĘTU I OPROGRAMOWANIA.

1. Sprzęt przetwarzający zbiory danych osobowych w Szpitalu składa się z:
a. serwerów z macierzowym systemem dysków,
b. komputerów stacjonarnych i przenośnych,
c. w sieci wewnętrznej wykorzystywane są switche; stosuje się także oddzielne zasilanie serwerów i podtrzymywanie ich zasilania przez urządzenia UPS,
d. dostęp do sieci Internet jest zabezpieczony poprzez router z funkcją Firewall
2. serwery, o którym mowa w ust. 1. pkt. a. są zamontowane w wyznaczonym pomieszczeniu wydzielonym z powierzchni biurowej, do którego dostęp mają tylko osoby upoważnione przez Inspektora Ochrony Danych.
3. Serwery służące do przetwarzania i przechowywania danych osobowych w systemie, podlegają zabezpieczeniu przed utratą, uszkodzeniem lub zniszczeniem danych na skutek awarii zasilania lub zakłóceń w sieci zasilającej poprzez podłączenie do odpowiednich urządzeń zasilających UPS.
4. Gniazda zasilania sieci są odpowiednio oznakowane lub wykonane standardowo.
5. Ekrany monitorów są wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu (nie więcej niż 600 sekund) od ostatniego użycia komputera.
6. Arkusze kalkulacyjne i inne pliki zawierające dane osobowe są zabezpieczone poprzez wbudowane środki ochrony – hasła ustalane na poziomie aplikacji/dokumentu/serwera plików.
7. BIOS komputerów PC jest zabezpieczony hasłem przed możliwością dokonywania zmian w konfiguracji komputera. Dodatkowym zabezpieczeniem jest brak urządzeń pamięci zewnętrznych lub ich zablokowanie w BIOS oraz na poziomie systemu operacyjnego, lub oprogramowania służącego do autoryzacji nośników pamięci zewnętrznej.
8. Komputery przenośne posiadają hasło zabezpieczające przed uruchomieniem komputera przez osoby nieupoważnione.
9. Dostęp do sieci wewnętrznej jest możliwy tylko z autoryzowanych komputerów.
10. Programy zainstalowane na komputerach stacjonarnych służących do przetwarzania danych osobowych są użytkowane z zachowaniem praw autorskich i powinny posiadać licencje.
11. Potrzebę instalacji oprogramowania systemowego oraz oprogramowania służącego do przetwarzania danych osobowych, o których mowa w ust. 1. sygnalizuje Administratorowi Administrator Systemów Informatycznych (ewentualnie inna wskazana przez niego osoba).
12. Inspektor Ochrony Danych zobowiązany jest zgłaszać Administratorowi propozycje w zakresie wyposażenia systemu w rozwiązania umożliwiające uwierzytelnianie użytkowników oraz dokonywanie kontroli dostępu do danych osobowych.
13. Używanie sprzętu komputerowego w trakcie przetwarzania danych osobowych do innych celów jest zabronione. Nieuprawniony użytkownik ma zablokowany dostęp do zasobów sprzętowych i programowych.

C. WYKAZ PROGRAMÓW BIZNESOWYCH

1. Wykaz programów biznesowych:
    a. Eskulap

b. Enova,
c. MS WINDOWS 10,
d. MS WiNDOWS Serwer,
e. Płatnik,
f. Microsoft Outlook,
g. Mozilla Thundirbird
h. Microsoft Office,
i. Microsoft Access,
j. Aplikacje własne z bazą danych access (PST – laboratorium; SPIRO_akcja – ambulans rtg; Archiwum_x – archiwizacja w składnicy akt z oddziałów, PCR – wyniki testów Covid-19, SEROLOGIA).
k. Calisia (Maksus, fiskus, kadrus) – program kadrowo, księgowo płacowy sprzed 2016 r.
l. Alteris PACS
m. System RIS i PACS Alteris w ambulansie (oddzielna instancja pacs)
n. Program reportserver

ROZDZIAŁ V.

PRZEGLĄD I KONSERWACJA SYSTEMU PRZETWARZAJĄCEGO DANE I SPRZĘTU KOMPUTEROWEGO

1. Sprzęt komputerowy powinien być użytkowany w sposób odpowiedni, tzn. zabezpieczony przed:
- strąceniem ze stołu,
- zalaniem napojem,
- wyrwaniem i/lub uszkodzeniem kabli.

Zakazane jest zakrywanie otworów wentylacyjnych komputera.

2. Min raz na pół Administrator Systemu Informatycznego dokonuje kompleksowej konserwacji systemu wraz ze sprawdzeniem zabezpieczenia systemu od strony Internetu i sieci lokalnej oraz uaktualniania komponentów. Kompleksowa kontrola służy sprawdzeniu czy na wszystkich urządzeniach aktualizacje systemu oraz zabezpieczeń są wykonywane na bieżąco.
3. Bieżących przeglądów i konserwacji sprzętu dokonują użytkownicy. W razie jakiejkolwiek awarii lub usterki powodującej brak możliwości korzystania z infrastruktury komputerowej użytkownicy są zobowiązani do niezwłocznego poinformowania o tym Administratora Systemu Informatycznego.
4. Administrator Systemu Informatycznego na bieżąco kontroluje podstawowe parametry systemu informatycznego, a w szczególności:
- stan dysków twardych,
- stan lokalnej sieci komputerowej,
- dostęp do Internetu,
- logi i komunikaty serwerów,
- ilość wolnego miejsca na nośnikach przeznaczonych do tworzenia kopii awaryjnych,
- aktualność stosowanych wersji oprogramowania,
- stan zasilaczy awaryjnych,

- stan centrali telefonicznych.

5. Prace dotyczące przeglądów, konserwacji i napraw inne niż określone w niniejszym rozdziale, wymagające zaangażowania autoryzowanych firm zewnętrznych, są wykonywane przez uprawnionych przedstawicieli tych firm pod nadzorem Administratora Systemów Informatycznych, bez dostępu do rzeczywistych danych osobowych.
6. W wyjątkowych sytuacjach, tj. w przypadku konieczności dostępu do informacji zastrzeżonych przez serwisantów, podpisują oni specjalny dokument o zachowaniu poufności.
7. Urządzenia komputerowe, dyski twarde lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu informacji zastrzeżonych lub naprawia się je pod nadzorem Administratora Systemu Informatycznego lub osoby przez niego upoważnionej.
8. Mechanizmy zapewniające nieprzerwane działanie systemu w przypadku awarii w tym zasilania, zostały opisane w procedurze Polityka Ciągłości Działania - Planach Awaryjnych.
9. Nadzór nad instalowaniem, sprawnym funkcjonowaniem i wymianą uszkodzonych urządzeń oraz oprogramowania sprawuje Administrator Systemów Informatycznych lub osoba przez niego upoważniona.
10. Zabronione jest używanie prywatnych nośników informacji (dyskietek, płyt CD, pamięci flash itp.)
11. Zabroniona jest zmiana konfiguracji sprzętowej i programowej komputera.
12. Zabronione jest samowolne instalowanie dodatkowego oprogramowania (np. gier, wygaszaczy ekranu, programów typu freeware itp.).
13. Zabronione jest instalowanie lub wyjmowanie części komputerowych.

ROZDZIAŁ VI.

OCHRONA SYSTEMU INFORMATYCZNEGO PRZED WIRUSAMI KOMPUTEROWYMI

1. Komputery, na których odbywa się przetwarzanie danych osobowych są okresowo sprawdzane przynajmniej jednym programem antywirusowym.
2. Każdy użytkownik sieci informatycznej powinien unikać wymiany plików pocztą elektroniczną z nieznanymi nadawcami i o podejrzanym temacie.
3. Skrzynki pocztowe posiadają wyłącznie uprawnieni użytkownicy. Pracownicy nie posiadający uprawnień nie posiadają skrzynek pocztowych.
4. Po udostępnieniu skrzynki pocztowej pracownik zobowiązany jest do regularnego, co najmniej raz dziennie, jej przeglądania. Poczta elektroniczna może być wykorzystywana wyłącznie w celach służbowych
5. Połączenie sieci informatycznej Szpitala z siecią Internet jest chronione za pomocą systemu firewall. Wykorzystywanie tego połączenia do celów nie związanych z działalnością firmy jest zabronione; w szczególności zabronione jest ściąganie plików chronionych prawem autorskim (filmy, muzyka, zdjęcia) oraz oprogramowania.
6. Nowe wersje oprogramowania antywirusowego Administrator Systemu Informatycznego instaluje niezwłocznie po ich otrzymaniu.
7. Nadzór nad instalowaniem nowego oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje Administrator Systemów Informatycznych lub osoby przez niego upoważnione.
8. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych. Szczególnej kontroli podlegają nośniki otrzymywane z zewnątrz.

9. W razie stwierdzenia wirusa, program antywirusowy usuwa wirusa, nie dopuszczając do zainfekowania systemu.
10. W sytuacji stwierdzenia przez użytkownika obecności wirusa, którego nie usunął program antywirusowy, użytkownik systemu obowiązany jest poinformować niezwłocznie o tym fakcie Administratora Systemu Informatycznego.
11. Administrator Systemu Informatycznego usuwa wirusa oraz informuje Inspektora Ochrony Danych o dokonanych czynnościach.
12. W przypadku, o którym mowa w ust. 11 Administrator Systemu Informatycznego odpowiada za usunięcie wirusa.
13. W razie niemożności usunięcia wirusa, Administrator Systemu Informatycznego po poinformowaniu Inspektora Ochrony Danych może skorzystać, za zgodą Administratora, z usług zewnętrznych specjalistów w tej dziedzinie.
14. W sytuacji korzystania z usług osób, o których mowa w ust. 14 należy podjąć działania uniemożliwiające tym osobom dostęp do danych osobowych.
15. W przypadku korzystania z usług osób, o których mowa w ust. 14 odpowiednie zastosowanie mają ust. 5-8 rozdziału IV oraz rozdziału X.
16. Specjaliści, o których mowa ust. 14 mogą dokonywać operacji na zainfekowanym komputerze wyłącznie pod opieką Administratora Systemów Informatycznych, lub upoważnionej przez niego osoby.
17. Po usunięciu wirusa Administrator Systemu Informatycznego we współpracy z Inspektorem Ochrony Danych sprawdza zainfekowany system informatyczny oraz przywraca go do pełnej funkcjonalności i sprawności.
18. Administrator Systemu Informatycznego - jeżeli zachodzi taka konieczność - powinien zaproponować zakup nowego programu antywirusowego Administratorowi.
19. Administrator Systemu Informatycznego sporządza raport o wystąpieniu wirusa. Raport winien zawierać następujące informacje:
    a. nazwę wirusa,
    b. datę wykrycia wirusa,
    c. miejscu zainfekowania,
    d. pochodzenie nośnika.
20. Raport przekazywany jest Inspektorowi Ochrony Danych wraz z wnioskami, stosownymi do zaistniałej sytuacji.
21. Inspektor Ochrony Danych prowadzi wykaz przypadków zainfekowania komputerów i nośników wykorzystywanych do przetwarzania danych osobowych w systemie w ramach Polityki Zarządzania Incydentami Bezpieczeństwa.
22. Procedura wyrażona w paragrafach powyższych niniejszego rozdziału ma zastosowanie także do przypadków awarii systemu spowodowanych błędem programu bądź użytkowników.

ROZDZIAŁ VII.

PROCEDURY ROZPOCZĘCIA I ZAKOŃCZENIA PRACY W SYSTEMIE

1. Stanowiska pracy powinny być tak usytuowane, by uniemożliwiać zapoznanie się z danymi osobowymi przez osoby trzecie. W przypadku wystąpienia sytuacji, gdy osoba nieuprawniona może mieć wgląd w dane wyświetlane na ekranie komputera niedozwolone jest przeglądanie informacji zawierających dane osobowe.
2. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić komputer i stanowisko pracy ze zwróceniem uwagi, czy nie zaszła jakakolwiek ingerencja, w szczególności czy nie odnotowano okoliczności wskazujących na naruszenie bezpieczeństwa danych osobowych.
3. O naruszeniu bezpieczeństwa danych mogą świadczyć w szczególności takie sytuacje jak:
   a) Brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych,
   b) Brak możliwości zalogowania się przez Użytkownika pomimo użycia właściwego loginu i hasła,
   c) Wykrycie na stanowisku komputerowym Użytkownika narzędzi programowych np. wirusów komputerowych, robaków, rootkit-ów, trojan-ów,
   d) Stwierdzenie fizycznej ingerencji w stanowisko komputerowe Użytkownika,
   e) Zamontowanie lub znajdowanie się na stanowisku komputerowym nowego, nieznanego urządzenia (narzędzi sprzętowych) np. przejściówki, w szczególności keyloggera sprzętowego, kamery, urządzeń podsłuchowych.
4. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie systemu, pracownik obowiązany jest niezwłocznie zawiadomić Administratora Systemu Informatycznego oraz Inspektora Ochrony Danych lub Administratora.
5. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:
   a) Włączenia stacji roboczej
   b) Uwierzytelnienia się („zalogowania") w systemie za pomocą identyfikatora i hasła.
6. Administrator Systemu Informatycznego ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania informując o nich Inspektora Ochrony Danych.
7. Kończąc pracę, pracownik obowiązany jest do:
   a. wylogowania się z systemu, a następnie wyłączenia sprzętu komputerowego,
   b. zabezpieczenia stanowiska pracy, w szczególności wszelkiej dokumentacji oraz nośników magnetycznych i optycznych, na których znajdują się dane osobowe i umieszczenia ich w wyznaczonym miejscu.
8. Przed opuszczeniem stanowiska pracy, trwającym do 30 minut, użytkownik systemu obowiązany jest zablokować komputer lub poczekać, aż zaktywizuje się wygaszacz ekranu chroniony hasłem.
9. W przypadku opuszczenia stanowiska pracy (wstrzymania pracy ze stacją roboczą) użytkownik zobowiązany jest zabezpieczyć dostęp do systemu informatycznego poprzez „zablokowanie komputera" czyli zaktywizowanie wygaszacza ekranu poprzez naciśnięcie klawiszy CTRL+ALT+DEL i wybranie opcji „Zablokuj". System informatyczny jest skonfigurowany tak, że ponowne odblokowanie komputera będzie możliwe dopiero po podaniu prawidłowego hasła użytkownika.
10. Niedopuszczalne jest przechowywanie danych oraz korzystanie z innego konta użytkownika niż własne. W szczególności niedopuszczalne jest podawanie współpracownikom danych uwierzytelniania, korzystanie z tak otrzymanych danych oraz praca w systemie informatycznym na koncie innego użytkownika.

11. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy przed dostępem osób nieupoważnionych, w szczególności zabezpieczając wszelkie nośniki informacji, dokumenty w postaci papierowej oraz wydruki zawierające dane osobowe.
12. W przypadku, gdy przerwa w pracy z systemem może trwać dłużej niż 30 minut, użytkownik systemu obowiązany jest wyłączyć komputer przeznaczony do pracy w systemie.
13. W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania („logowaniu się" w systemie) np. braku możliwości zalogowania się na własne konto lub w przypadku stwierdzenia fizycznej ingerencji w przetwarzane dane lub użytkowane narzędzie programowe lub sprzętowe użytkownik niezwłocznie powiadamia o nich Administratora Systemu Informatycznego a ten, po sprawdzeniu zasadności zgłoszenia i w razie konieczności Inspektora Ochrony Danych lub Administratora.
14. Wszyscy użytkownicy systemu podlegają szkoleniu z zakresu „przyłączania się" (logowania) do sieci komputerowej Szpitala i zakończenia pracy z systemem.

ROZDZIAŁ VIII.

ZASADY ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DOSTĘPEM OSÓB NIEUPRAWNIONYCH

1. Kontrola dostępu i autoryzacja użytkowników następują poprzez podanie identyfikatora i hasła przy logowaniu się do pracy z systemem.
2. Każdy użytkownik otrzymuje identyfikator uprawniający do wykonywania czynności zgodnie z zakresem powierzonych mu obowiązków, które wyznaczają poziom jego uprawnień.
3. Monitory komputerów przeznaczonych do przetwarzania danych osobowych w systemie informatycznym muszą być usytuowane w taki sposób, aby uniemożliwiały osobom nieupoważnionym odczytanie informacji aktualnie wyświetlanej na ekranie.
4. Sposób realizacji wymogu zapisania w systemie informacji o odbiorcach, którym dane osobowe zostały udostępnione - do rejestracji informacji o udostępnieniu danych osobowych wykorzystywany powinien być dedykowany do tego system informatyczny, który umożliwia rejestrację tego jakie zbiory i jaki zakres danych osobowych zostały udostępnione, komu, kiedy i na jakiej podstawie.

ROZDZIAŁ IX.

TRYB WYMIANY DANYCH OSOBOWYCH

1. Dane osobowe gromadzone w systemach informatycznych Szpitala wymieniane są pomiędzy użytkownikami przy użyciu bezpiecznego kanału komunikacji elektronicznej lub w formie papierowej.
2. Nośniki magnetyczne użytkownicy przesyłają pocztą poleconą bądź kurierską lub dostarczają osobiście do rąk własnych adresatów.
3. Każdy nośnik powinien być odpowiednio oznakowany i opisany.
4. Przekazywane dane osobowe kanałami: poczta / CD są każdorazowo szyfrowane. Za szyfrowanie danych odpowiada użytkownik wysyłający dane. Wskazane minimalne zabezpieczenia to spakowanie pliku danymi do archiwum zabezpieczonym hasłem oraz przesłanie hasła oddzielna wiadomością (najlepiej korzystając z innego medium komunikacyjnego, np. mail i wiadomość sms z telefonu służbowego)

ROZDZIAŁ X.

SPOSÓB I CZĘSTOTLIWOŚĆ TWORZENIA I PRZECHOWYWANIA KOPII ZAPASOWYCH /AWARYJNYCH/

1. Zbiory danych systemu są przechowywane na dysku twardym w komputerze do tego przeznaczonym /serwerze/, a ponadto są składowane na kopiach zapasowych (awaryjnych).
2. Do obowiązków Administratora Systemów Informatycznych należy archiwizowanie (tworzenie kopii zapasowych):
   a. baz danych,
   b. danych finansowych
   c. aplikacji użytkowych i katalogów działowych
   d. folderów domowych użytkowników
3. Do przechowywania backupów używane są urządzenia typu NAS oraz backup przechowywany jest w innej lokalizacji.

   Kopie zapasowe tworzone są zgodnie z „Wykazem procedur archiwizacji danych informatycznych" stanowiącym załącznik do niniejszej polityki.

   Kopie zapasowe (awaryjne), które uległy uszkodzeniu lub zdezaktualizowały się podlegają natychmiastowemu nieodwracalnemu zniszczeniu.

   Niszczenia kopii zapasowych, na nośnikach magnetycznych i optycznych, o których mowa w ust. 7., dokonuje użytkownik w obecności Administratora Systemu Informatycznego lub osoby przez niego upoważnionej.

   Z nośników magnetycznych 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.

   Dane zawarte na nośnikach optycznych należy usuwać poprzez całkowite zniszczenie nośnika.

   Tryb postępowania z archiwalnymi kopiami zapasowymi, został określony w kolejnym rozdziale.

ROZDZIAŁ XI.

ARCHIWIZOWANIE I LIKWIDACJA ZBIORÓW DANYCH

1. Celem syntetycznego ujęcia procedury archiwizacyjnej i likwidacyjnej w przedmiotowym rozdziale ujęto sposób archiwizacji i likwidacji zbiorów zarówno w systemie informatycznym jak i kartotekach ewidencyjnych w wersjach papierowych.
2. Wydruki i dokumenty papierowe zawierające dane osobowe przechowywane powinny być chronione przed dostępem osób nieuprawnionych, wyłącznie w odrębnych zamykanych szafach. Niedozwolone jest pozostawianie wydruków, nawet tymczasowo, w miejscach, gdzie istnieje możliwość dostępu do nich osób nieuprawnionych.
3. Osoba zatrudniona przy przetwarzaniu danych osobowych, sporządzająca wydruk zawierający dane osobowe ma obowiązek na bieżąco sprawdzać przydatność wydruku w wykonywanej pracy, a w przypadku jego nieprzydatności – niezwłocznie wydruk zniszczyć w niszczarce.
4. Zbiory danych na nośnikach magnetycznych lub optycznych, przekazanych przez kontrahenta do Szpitala lub pozyskanych bezpośrednio przez Szpital w trakcie obsługi, archiwizowana jest do czasu zakończenia przetwarzania danych, określonego w umowie zawartej z kontrahentem.

5. Po tym okresie cała dokumentacja papierowa zawierająca dane osobowe, związana ze świadczeniem usług przekazywana jest do właściwego Administratora powierzającego dane osobowe do przetwarzania lub za jego zgodą niszczona zgodnie z niniejszą Polityką.
6. Zabrania się trwałego przechowywania danych osobowych na nośnikach magnetycznych i optycznych (np. taśma, pendrive, płyta CD/DVD, dysk przenośny) wynoszonych poza siedzibę firmy. Dopuszczalne jest tymczasowe zapisanie danych na takich nośnikach w celu np. przeniesienia danych, ale pod warunkiem zapewnienia bezpieczeństwa tego nośnika i skutecznego usunięcia ich niezwłocznie po tym jak cel ich nagrania zostanie osiągnięty. Jeśli dane na nośnikach mają być przechowywane dłużej, bez stałej kontroli użytkownika muszą być zapisane w postaci zaszyfrowanej, tak by uniemożliwić ich odczytanie osobom niepowołanym.
7. Dane przechowywane na urządzeniach mobilnych powinny być trwale zaszyfrowane. Dotyczy to w szczególności komputerów przenośnych (notebook) oraz smartfonów. Dane niezbędne do odblokowania dostępu do zaszyfrowanego nośnika (kod PIN) powinny być szczególnie chronione przez użytkownika.
8. Po okresie, o którym mowa w ust. 4., zbiór danych na nośnikach magnetycznych zawierający dane osobowe podlega trwałemu usunięciu lub takiej modyfikacji (anonimizacji lub pseudonimizacji), która nie pozwoli na ustalenie tożsamości osób, których dane dotyczyły.
9. Fizyczna likwidacja zniszczonych lub niepotrzebnych magnetycznych i optycznych nośników informatycznych z danymi osobowymi powinny być dokonany w sposób uniemożliwiający odczyt danych osobowych.
10. Decyzję o likwidacji danych osobowych podejmuje, na wniosek Inspektora Ochrony Danych, Administrator.
11. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów archiwalnych, Inspektor Ochrony Danych sporządza protokół, w którym zamieszcza następujące informacje:

a) data dokonania likwidacji,
b) przedmiot likwidacji (nośniki, kartoteka ewidencyjna),
c) przedział czasowy likwidowanego archiwum,
d) podpisy osób dokonujących i obecnych przy likwidacji archiwum.

12. W przypadku, gdy zaistnieje potrzeba naprawy lub wymiany sprzętu komputerowego służącego do przechowywania i przetwarzania danych osobowych w systemie należy usunąć z dysku twardego wszystkie dane.
13. Procedurę kasowania danych z nośnika należy przeprowadzić za pomocą oprogramowania służącego do nieodwracalnego usuwania danych z dysku –poprzez przynajmniej 3 krotne nadpisanie bitu na dysku za pomocą narzedzi low level format.
14. Jeżeli dysk twardy jest uszkodzony i nie ma możliwości skasowania z niego danych należy wymontować go z komputera i zniszczyć.
15. Niszczenie dysku polega na trwałym uszkodzeniu nośnika danych poprzez wymontowanie talerza dysku, jego rozmagnesowanie, zarysowanie oraz połamanie.
16. Likwidacja danych osobowych odbywa się za zgodą i w obecności Inspektora Ochrony Danych lub osoby przez niego upoważnionej.
17. Dopuszczalne jest zlecenie/powierzenie niszczenia wszelkich nośników danych osobowych wyspecjalizowanym podmiotom zewnętrznym. Podstawą przekazania danych do zniszczenia innemu podmiotowi powinna być w każdym przypadku umowa zawarta na piśmie.

ROZDZIAŁ XII.

PROCES POSTĘPOWANIA W PRZYPADKU AWARII SERWERA I/LUB SYSTEMU INFORMATYCZNEGO

1. W przypadku awarii serwera i/lub systemu produkcyjnego powoływany jest komitet kryzysowy w składzie:
a. Administrator Systemu Informatycznego (Dział IT)
b. Inspektor Ochrony Danych
2. Pierwszym podejmowanym krokiem jest zawieszenie uprawnień użytkowników i zakomunikowanie o czasowym zablokowaniu dostępu do serwera/systemu.
3. Później ustalane jest źródło awarii i obszar uszkodzeń.
4. Następnie podejmowane są działania w celu usunięcia awarii i próby naprawy serwera/systemu.
5. Kolejnym krokiem jest sprawdzanie poprawności i spójności systemów i zbiorów danych.
6. Finalnie serwer/system oraz zbiory danych poddawane są procedurze testowania i dopiero po stwierdzeniu poprawności jego działania następuje przywrócenie uprawnień dla użytkowników i poinformowanie ich o możliwości bezpiecznego przetwarzania danych.
7. W przypadku nieudanej próby naprawy serwera następuje bezzwłoczne przejście na serwer zapasowy. Uszkodzony serwer podlega bezzwłocznej naprawie w siedzibie firmy.

   Administrator Systemu Informatycznego sporządza raport, który przekazuje Administratorowi i Inspektorowi Ochrony Danych.
8. Punkty 9-12 określają zasady postępowania w stosunku do osób, które dopuściły się zaniedbań związanych z zapewnieniem bezpieczeństwa przetwarzania danych.
9. W sytuacji, gdy zagrożenie bezpieczeństwa zaistniało w wyniku działań osoby zatrudnionej przy przetwarzaniu danych, Inspektor Ochrony Danych występuje o pozbawienie praw dostępu do danych osobowych dla tej osoby.
10. Identyfikator osoby, która utraciła uprawnienia dostępu do danych jest niezwłocznie unieważniany w systemie informatycznym. Hasło takiej osoby jest unieważniane, jak również podejmowane są wszelkie czynności, których celem jest zapobieżenie dalszemu dostępowi tej osoby do danych.
11. Jeżeli zachodzi podejrzenie, że naruszenie lub powstałe niebezpieczeństwo naruszenia ochrony danych jest wynikiem czynu karalnego, Inspektor Ochrony Danych zawiadamia o powyższych okolicznościach właściwy organ ścigania.
12. Jeżeli okoliczności faktycznie wskazują na konieczność natychmiastowej interwencji organów ścigania, zawiadomienia takiego dokonać może osoba zatrudniona przy przetwarzaniu danych (operator danych), o czym niezwłocznie powiadomi Inspektora Ochrony Danych.
13. Serwery chronione są przed awarią zasilania poprzez zasilacze awaryjne, które zapewniają bieżącą kontrolę i korektę parametrów zasilania, jak również w wypadku całkowitego zaniku napięcia zapewniają utrzymanie jego poziomu do czasu bezpiecznego wyłączenia serwerów.

ROZDZIAŁ XIII.

POSTANOWIENIA KOŃCOWE

1. Polityka Zarządzania Systemem Teleinformatycznym jest dokumentem wewnętrznym i stanowi integralną część Polityk Ochrony Danych w rozumieniu Ogólnego Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 o ochronie danych osobowych.
2. Polityka Zarządzania Systemem Teleinformatycznym nie może być udostępniania osobom postronnym w żadnej formie.
3. Inspektor Ochrony Danych lub osoby przez niego upoważnione, udostępnia do wglądu, każdej osobie zatrudnionej przy przetwarzaniu danych Politykę Zarządzania Systemem Teleinformatycznym, celem zapoznania się i stosowania.
4. W sprawach nieuregulowanych w Polityce Zarządzania Systemem Teleinformatycznym mają zastosowanie przepisy Ogólnego Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 o ochronie danych osobowych oraz odpowiednich przepisów wykonawczych.