Zarządzenie nr 30/2018
Dyrektora Wojewódzkiego Centrum Psychiatrii Długoterminowej
w Stroniu Śląskim SP ZOZ
z dnia 22 maja 2018 roku

w sprawie wprowadzenia POLITYKA BEZPIECZEŃSTWA przetwarzania i ochrony danych osobowych w Wojewódzkim Centrum Psychiatrii Długoterminowej w Stroniu Śląskim SP ZOZ.

Na podstawie § 5 pkt 1, § 6 ust. 1 Statutu Wojewódzkiego Centrum Psychiatrii Długoterminowej- załącznik do uchwały Sejmiku Województwa Dolnośląskiego z dnia 20 grudnia 2012 r., nr XXX/839/12, zarządza się, co następuje:

§ 1.

Zatwierdza się i wprowadza się POLITYKA BEZPIECZEŃSTWA przetwarzania i ochrony danych osobowych w Wojewódzkim Centrum Psychiatrii Długoterminowej w Stroniu Śląskim SP ZOZ.

§ 2.

Treść POLITYKI BEZPIECZEŃSTWA zawiera załącznik nr 1 do niniejszego zarządzenia.

§ 3.

Uchyla się zarządzenie nr 21/2016 Dyrektora Wojewódzkiego Centrum Psychiatrii Długoterminowej SPZOZ w Stroniu Śląskim z dnia 18 kwietnia 2016 r. w sprawie wprowadzenia Regulaminu przechowywania i ochrony danych osobowych w Wojewódzkim Centrum Psychiatrii Długoterminowej SPZOZ w Stroniu Śląskim.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania, z mocą obowiązującą od dnia 25 maja 2018 r.

DYREKTOR CENTRUM

Joanna Chromiec

Załącznik nr 1 do Zarządzenia Dyrektora WCPD SP ZOZ z dnia 22 maja 2018 r.

POLITYKA BEZPIECZEŃSTWA
przetwarzania i ochrony danych osobowych w Wojewódzkim Centrum Psychiatrii Długoterminowej w Stroniu Śląskim SP ZOZ.

Rozdział 1
Postanowienia ogólne

§ 1

Celem Polityki bezpieczeństwa przetwarzania i ochrony danych osobowych, zwanej dalej „Polityką bezpieczeństwa" w Wojewódzkim Centrum Psychiatrii Długoterminowej w Stroniu Śląskim, Samodzielny Publiczny Zakład Opieki Zdrowotnej, zwanej dalej „Jednostką", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

§ 2

Polityka bezpieczeństwa została opracowana w oparciu o wymagania zawarte w:
1) rozporządzeniu 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 /Dz. Urz. UE.L nr 119;
2) ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000).

§ 3

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności.

§ 4

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Jednostce rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest akceptowalna wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
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 tylko tej osobie;
4) integralność systemu- rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
5) dostępność informacji- rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
6) zarządzanie ryzykiem- rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

Rozdział 2
Definicje

§ 5

Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

1) **administrator danych osobowych-** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,

2) **inspektor ochrony danych-** osoba wyznaczona przez administratora danych osobowych, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych,

3) **ustawa-** ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000),

4) **RODO-** 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 /Dz. Urz. UE.L nr 119,

5) **dane osobowe-** wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,

6) **system informatyczny-** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,

7) **system tradycyjny-** zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze,

8) **zabezpieczenie danych w systemie informatycznym-** wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

9) **administrator systemu informatycznego-** osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi,

10) **odbiorca** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia,

11) **strona trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe,

12) **identyfikator użytkownika (login)-** ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

13) **hasło-** ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Rozdział 3
Zakres stosowania

§ 6

1. W Organizacji przetwarzane są dane osobowe pacjentów oraz pracowników, zebrane w zbiorach danych osobowych.

2. Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.
3. Polityka bezpieczeństwa zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.
4. Innymi dokumentami regulującymi ochronę danych osobowych w Jednostce są:
1) Rejestr Czynności Przetwarzania Danych Osobowych,
2) Ocena skutków planowanych operacji,
3) Plan postępowania z ryzykiem dla ochrony danych osobowych,
4) Procedura postępowania na wypadek naruszenia ochrony danych osobowych,
5) Ewidencja osób upoważnionych do przetwarzania danych osobowych.

§ 7

Politykę bezpieczeństwa stosuje się w szczególności do:
1) danych osobowych przetwarzanych w systemie: InfoMedica- (Kadry, Płace, Finanse- Księgowość, Izba przyjęć, Poradnia, Rozliczenia z NFZ, Apteczka oddziałowa, Apteka), *Płatnik, Microsoft Office, OpenOffice itp*,
2) wszystkich informacji dotyczących danych osobowych pacjentów oraz pracowników Jednostki,
3) odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia,
4) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
5) rejestru osób trzecich (pracowników) mających upoważnienia administratora danych osobowych do przetwarzania danych osobowych,
6) innych dokumentów zawierających dane osobowe.

§ 8

1. Zakresy ochrony danych osobowych określone przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty mają zastosowanie do:
1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie,
2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
3) wszystkich pracowników, stażystów i innych osób mających dostęp do informacji podlegających ochronie.
2. Do stosowania zasad określonych w Polityce bezpieczeństwa oraz w dokumentach z nią związanych, zobowiązani są wszyscy pracownicy, stażyści oraz inne osoby mające dostęp do danych osobowych podlegających ochronie.

Rozdział 4
Wykaz zbiorów danych osobowych

§ 9

Dane osobowe gromadzone są w zbiorach:
1) Ewidencja osób upoważnionych do przetwarzania danych osobowych,
2) imię, nazwisko/nazwisko rodowe,
3) adres zamieszkania/zameldowania lub pobytu,

4) zawód,
5) imiona i nazwiska rodziców/opiekuna/kuratora i ich dane teleadresowe,
6) numer ewidencyjny PESEL,
7) wykształcenie,
8) numer Identyfikacji Podatkowej NIP,
9) decyzje ZUS, Pomocy Społecznej, Urzędów Pracy w sprawie przyznanych świadczeń,
10) seria i nr dowodu osobistego/inny dokument tożsamości,
11) data i miejsce urodzenia,
12) miejsce pracy,
13) numer telefonu,
14) pochodzenie rasowe,
15) przekonania filozoficzne,
16) stan zdrowia w tym dane niezbędne do zawarcia umowy dobrowolnego ubezpieczenia,
17) pochodzenie etniczne,
18) przynależność wyznaniowa,
19) kod genetyczny,
20) poglądy polityczne,
21) przynależność partyjna,
22) nałogi i uzależnienia,
23) przekonania religijne,
24) przynależność związkowa,
25) życie seksualne,
26) nr rachunku bankowego,
27) uprawnienia zawodowe,
28) ewidencja czasu pracy pracowników,
29) dane o przyznanych karach, nagrodach i potrąceniach, zajęciach komorniczych pracowników,
30) dane o absencji pracowników (urlopy okolicznościowe, urlopy wypoczynkowe, choroby, rehabilitacja itp.),
31) dane niezbędne w celu wypłaty świadczeń z ZFŚS,
32) dane o niepełnosprawności ,
33) dane o otrzymywanym wynagrodzeniu,
34) dane telemetryczne,
35) rejestr korespondencji i paczek,
36) ewidencja osób upoważnionych do przetwarzania danych osobowych,
37) rejestr wydanej odzieży ochronnej i środków ochrony indywidualnej,
38) rejestr delegacji służbowych,
39) deklaracje ubezpieczeniowe pracowników,
40) rejestr wypadków (rejestr zakłóć),
41) rejestr mów cywilnoprawnych,
42) dokumenty archiwalne (archiwum),
43) karty zasiłkowe,
44) karty zarobkowe,
45) informacje o zarobkach rocznych PIT- y,
46) ewidencja akt osobowych,
47) lista plac,

48) deklaracje ubezpieczeniowe pracowników (dokumentacja ubezpieczeniowa).

Rozdział 5
Wykaz budynków, pomieszczeń, w których wykonywane są operacje przetwarzania danych osobowych

§ 10

Dane osobowe przetwarzane są w budynkach: przy ul. Sudeckiej 3A w Stroniu Śląskim i przy ul. Morawka 1 w Stroniu Śląskim, tj.:

1) budynek przy ul. Sudeckiej 3A

Budynek A:

Parter- 2, 22, 28, 29, 30, 32, Informacja/portiernia

I piętro – 2, 22, 28, 29, 30, 32

II piętro – 1, 2, 3, 4, 6, 7, 8, 9, 10, 12, 13, 14, 15, 17, 18, 19, 21, 27

Budynek B:

Piwnica – 025, 042

Parter – 12, 19, 21, 22, 23, 25, 27, 28, 30, 37

I piętro – 112, 119, 121, 122, 123, 127, 129, 136

II piętro – 218, 224, 226, 227, 228, 230, 232, 234, 242, 257, 258

2) budynek przy ul. Morawka 1- Archiwum oraz Poradnia Zdrowia Psychicznego.

Rozdział 6
Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

§ 11

W Jednostce przetwarza się dane osobowe z zastosowaniem następujących programów:

ZBIÓR DANYCH OSOBOWYCH	PROGRAM INFORMATYCZNY SŁUZĄCY DO PRZETWARZANIA ZBIORU DANYCH	STRUKTURA DANYCH
Pracownicy	infoMedica Kadry/Płace	PESEL/ NIP/ imię (imiona) i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ płeć/adres stały/ numer telefonu/ e-mail/ dowód osobisty (seria i nr, wydany przez, data wydania)/ imię ojca/ imię matki/ stan cywilny i rodzinny/ numer legitymacji służbowej/ posiada gospodarstwo rolne/ emeryt/ rencista/ obywatelstwo obce/ dane osoby kontaktowej/ wykształcenie/ nazwa szkoły i rok ukończenia/ staż pracy/ historia pracy/ warunki zatrudnienia/ wysokość wynagrodzenia/ukończone kursy/ kary i nagrody/ nieobecności w pracy/ informacja o karalności/ informacje o stanie zdrowia

	Płatnik	PESEL/ NIP/ imię/nazwisko/ adres/ data i miejsce urodzenia
	infoMedica Księgowość	PESEL/ NIP/ imię/nazwisko/ adres/ data i miejsce urodzenia/ numer konta bankowego
	infoMedica Środki trwałe	PESEL/ NIP/ imię/nazwisko/ adres/ data i miejsce urodzenia/ numer konta bankowego
	infoMedica Kasa	PESEL/ NIP/ imię/nazwisko/ adres/ data i miejsce urodzenia/ numer konta bankowego
Pacjenci	**MMEDICA**	PESEL/imię i nazwisko/ data i miejsce urodzenia/ płeć/adres stały /numer telefonu/ dowód osobisty (seria, numer i rodzaj, wydany przez, data wydania)/ Dane medyczne, data udzielenia świadczeń, nazwisko lekarza przyjmującego, rozpoznania, procedury wykonane.

Zbiory danych przetwarzanych tradycyjnie

ZBIÓR DANYCH OSOBOWYCH	DOKUMENTACJA SŁUZĄCA DO PRZETWARZANIA ZBIORU DANYCH	STRUKTURA DANYCH
	Akta osobowe	PESEL/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/płeć/adres stały/ numer telefonu/ e-mail/ dowód osobisty (seria i nr, wydany przez, data wydania)/ imię ojca/ imię matki/ stan cywilny i rodzinny/stosunek do służby wojskowej (dokument wojskowy, seria i numer, stopień wojskowy)/ numer legitymacji służbowej/ posiada gospodarstwo rolne/ emeryt/ rencista/ obywatelstwo obce/ osoba kontaktowa/ wykształcenie/ nazwa szkoły i rok ukończenia/ warunki zatrudnienia/ staż pracy/ historia pracy, kary, nagrody/ tytuł zawodowy/ zawód wyuczony i wykonywany/ uzyskane kwalifikacje/ nieobecności w pracy
	Ewidencja akt osobowych	imię i nazwisko/ data i miejsce urodzenia/ adres stały

Pracownicy	Orzeczenia lekarskie do celów sanitarno-epidemiologicznych	PESEL/ imię i nazwisko/ adres stały/ informacje o stanie zdrowia
	Dane niezbędne w celu wypłaty świadczeń z ZFŚS	imię i nazwisko/ adres stały/ wysokość zarobków
	Listy płac	PESEL/ imię i nazwisko/ stanowisko/ numer konta bankowego
	Karty zasiłkowe	PESEL/NIP/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały/okresy niezdolności do pracy
	Karty zarobkowe	PESEL/NIP/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały/wysokość zarobków/ warunki pracy (wymiar etatu, okres umowy)
	Informacje o zarobkach rocznych (PIT-y)	PESEL/NIP/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały/wysokość zarobków
	Zaświadczenia	PESEL/NIP/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały/wysokość zarobków/ warunki pracy
	Deklaracje ubezpieczeniowe pracowników (dokumentacja ubezpieczeniowa)	PESEL/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały/ informacje o stanie zdrowia
	Rejestr wypadków (w tym protokoły powypadkowe, rejestr zakłuć)	imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały/ informacje o stanie zdrowia

Rozdział 7
Sposób przepływu danych między poszczególnymi systemami, współpracy systemów informatycznych ze zbiorami danych

§ 12

Przepływ danych pomiędzy poszczególnymi systemami jest następujący:

KADRY -> PŁATNIK

Z aplikacji **miniInfoMedica kadry** do programu **Prokom Płatnik** przekazywane są dane dotyczące zarejestrowania i wyrejestrowania pracowników.

PŁACE -> PŁATNIK

Z aplikacji **miniInfoMedica płace** do programu **Prokom Płatnik** przekazywane są dane dotyczące składek na ubezpieczenia.

PŁACE -> BANK SPÓŁDZIELCZY w Strzelinie

Z programu **miniInfoMedica płace** do **Bank Spółdzielczy w Strzelinie** przekazywane są dane dotyczące należnych kwot przelewanych na konto pracowników pracowników. Przekazywanie poprzez import listy przelewów do aplikacji internetowej.

miniInfoMedica część biała

Moduł ROZLICZENIA – przekazywanie danych pacjentów niezbędnych do rozliczenia wykonanych świadczeń w Narodowym Funduszu Zdrowia.

ROZLICZENIA -> POSTAL ŚWIADCZENIOWDAWCY

Moduł kolejki oczekujących – przekazywanie do NFZ koleki osób do przyjęcia do Centrum. Przekazywane są dane rozliczeniowe do NPZ

Pozostałe programy są niezależne i posiadają samodzielne bazy danych.

Rozdział 8
Środki organizacyjne i techniczne zabezpieczenia danych osobowych

§ 13

1. Zabezpieczenia organizacyjne :

1) opracowano i wdrożono Politykę bezpieczeństwa przetwarzania danych osobowych,

2) sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Jednostce,

3) stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych,

4) opracowano i bieżąco prowadzi się rejestr czynności przetwarzania,

5) wyznaczono inspektora ochrony danych,

6) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych,

7) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,

8) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,

9) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,

10) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,

11) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści.

2. Zabezpieczenia techniczne :
1) wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą VIGOR 29/25.
2) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,
3) komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i hasła,
3. Środki ochrony fizycznej :
1) obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest alarmem w Archiwum,
2) obszar, na którym przetwarzane są dane osobowe objęty jest całodobowym monitoringiem,
3) urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach,
4) dokumenty i nośniki informacji zawierające dane osobowe przechowywane są w zamykanych na klucz szafach.

Rozdział 9
Zadania inspektora ochrony danych

§ 14

Do najważniejszych obowiązków inspektora ochrony danych należą:
1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO i ustawy o ochronie danych osobowych,
2) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki bezpieczeństwa i innymi dokumentami wewnętrznymi,
3) przeprowadzenie oceny skutków planowanej operacji przetwarzania dla ochrony danych osobowych, w przypadku, gdy organizacja wprowadza nowy rodzaj przetwarzania danych osobowych,
4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
5) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
6) nadzór nad bezpieczeństwem danych osobowych,
7) kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
8) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

Rozdział 10
Zadania informatyka

§ 15

Informatyk zatrudniony w Jednostce, odpowiedzialny jest w szczególności za:
1) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
2) optymalizację wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego,
3) instalacje i konfiguracje oprogramowania systemowego, sieciowego,
4) konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
5) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ

na bezpieczeństwo przetwarzania danych,
6) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
7) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
8) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
9) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
10) przyznawanie na wniosek administratora danych osobowych lub inspektora ochrony danych ściśle określonych praw dostępu do informacji w danym systemie,
11) wnioskowanie do administratora danych osobowych lub inspektora ochrony danych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
12) zarządzanie licencjami.

Rozdział 11
Sprawozdanie roczne z funkcjonowania systemu ochrony danych osobowych

§ 16

1. Corocznie do dnia 31 marca każdego roku inspektor ochrony danych przygotowuje sprawozdanie roczne z funkcjonowania systemu ochrony danych osobowych i przekazuje do administratora danych osobowych.
2. Sprawozdanie przygotowywane jest w formie pisemnej.

Rozdział 12
Postanowienia końcowe

§ 17

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada administrator danych osobowych lub inspektor ochrony danych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką bezpieczeństwa i innymi związanymi z nią dokumentami obowiązującymi u administratora danych osobowych.
4. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.