Polityka bezpieczeństwa przetwarzania danych osobowych w PoorSnap

WROCŁAW, 2017

I. Wstęp

§ 1

Celem Polityki Bezpieczeństwa przetwarzania danych osobowych w **PoorSnap**, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami *obowiązujących aktów prawnych,* sposobu przetwarzania w **PoorSnap** informacji zawierających dane osobowe, a przede wszystkim zapewnienie ochrony danych osobowych przetwarzanych w **PoorSnap** przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.

§ 2

Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzeniu 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. Opracowany dokument jest zgodny również z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.

§ 3

Obszarem przetwarzania danych osobowych w **PoorSnap** są wydzielone pomieszczenia w budynku, w którym mieści się Biuro, tj. budynek D1 przy ul. Plac Grunwaldzki 13, 50-377 Wrocław.

§ 4

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników.

§ 5

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w **PoorSnap** rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest 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.

§ 6

Administratorem Danych Osobowych przetwarzanych w **PoorSnap** jest Jan Kowalski legitymujący się dowodem osobistym o numerze AWK-1234

§ 7

Na Administratora Bezpieczeństwa Informacji w **PoorSnap** mianowana jest Joanna Nowak legitymujący się dowodem osobistym o numerze XYZ-345

II. Definicje

§ 8

Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:

1. **Polityka Bezpieczeństwa** - rozumie się przez to Politykę Bezpieczeństwa Danych Osobowych w **PoorSnap**;
2. **Administrator Danych Osobowych** - dalej jako Administrator danych; rozumie się przez to Jan Kowalski.
3. **Administrator Bezpieczeństwa Informacji (także ABI)** - rozumie się przez to osobę wyznaczoną przez Administratora Danych Osobowych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
4. **Biuro** - Biuro **PoorSnap;**
5. **Ustawa** - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz. 1182);
6. **Rozporządzenie** - rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024);
7. **Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
8. **Zbiór danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
9. **Baza danych osobowych** - zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe;
10. **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą.
11. **Przetwarzane 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;
12. **System informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
13. **System tradycyjny** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
14. **Zabezpieczenie danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
15. **Administrator systemu informatycznego** – rozumie się przez to osobę lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi w **PoorSnap;**

16. **Użytkownik -** rozumie się przez to upoważnionego przez Administratora danych lub Administratora Bezpieczeństwa Informacji, wyznaczonego do przetwarzania danych osobowych pracownika lub członka zarządu **PoorSnap**, który odbył stosowne szkolenie w zakresie ochrony tych danych.

III. Zakres zastosowania

§ 9

1. W **PoorSnap** przetwarzane są przede wszystkim informacje służące do sprzedaży i reklamacji produktów na urządzenia mobilne. Przechowywane są informacje o klientach potrzebne do wystawiania faktur takie jak imiona i nazwiska nabywcy, datę zakupu, nazwę towaru, numer podatkowy.
2. Informacje są przetwarzane i składowane zarówno w postaci dokumentacji tradycyjnej jak i elektronicznej.
3. Polityka Bezpieczeństwa zawiera dokumenty dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych.

§ 10

Politykę Bezpieczeństwa stosuję się przede wszystkim do:
1. Danych osobowych przetwarzanych w systemie: Płatnik, Microsoft Office, Microsoft SQL Server 2016, Systemu Reklamacji Użytkownika (**SRU**)
2. Wszystkich informacji dotyczących danych pracowników **PoorSnap,** w tym danych osobowych pracowników i treści zawieranych umów o pracę.
3. Wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji.
4. Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych.
5. Rejestru osób dopuszczonych do przetwarzania danych osobowych.
6. Innych dokumentów zawierających dane osobowe.

§ 11

Zakresy ochrony danych osobowych określone przez dokumenty Polityki Bezpieczeństwa mają zastosowanie do systemów informatycznych Izby, w których są przetwarzane dane osobowe, a w szczególności do:

- Wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;
- Wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
- Wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, stażystów i innych osób mających dostęp do informacji podlegających ochronie, w tym do członków zarządu **PoorSnap**.

2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie, w tym członkowie zarządu **PoorSnap**.

§ 12

Informacje niejawne nie są objęte zakresem niniejszej Polityki Bezpieczeństwa.

IV. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe oraz sposobów ich zabezpieczeń

§ 13

1. Polityka obowiązuje w **PoorSnap**, w pomieszczeniach lub częściach pomieszczeń, w których przetwarzane są dane osobowe, a których wykaz został zamieszczony poniżej.
2. **PoorSnap** mieści się pod adresem: budynek D1 przy ul. Plac Grunwaldzki 13, 50-377 Wrocław oraz w filii pod adresem: ul Andrzeja Potebni 1/23 51-677 Wrocław

1	Wykaz pomieszczeń, w których przetwarzane są dane osobowe (wskazanie konkretnych nr. pomieszczeń)	Sala 317.3 w budynku D1, oraz „Pokój Urzyna” na ul. Potebni
2	Wykaz pomieszczeń, w których znajdują się komputery stanowiące element systemu informatycznego	„Pokój Urzyna” na ul. Potebni
3	Wykaz pomieszczeń, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe)	Sala 317.2 w budynku D1.
4	Wykaz pomieszczeń, w których składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, dyski przenośne, uszkodzone komputery)	Nie są składowane, zajmuje się tym specjalistyczna firma zewnętrzna, która trwale niszczy nośniki.
5	Wykaz pomieszczeń archiwum	Sala 017 w budynku D1.
6	Wykaz programów, w których przetwarzane są dane osobowe	Płatnik, Microsoft Office, Microsoft SQL Server Management Studio 2016, Microsoft SQL Server 2016
7	Wykaz podmiotów zewnętrznych, które mają dostęp do danych osobowych lub je przetwarzają na podstawie podpisanych umów (np. informatyk) – nazwa firmy, imię, nazwisko, adres, funkcja.	Firma zewnętrzna zajmująca się niszczeniem uszkodzonych nośników danych „RM-RF”, Ryszard Stallman
8	Inne (proszę podać inne informacje dotyczące pomieszczeń, w których przetwarzane są dane osobowe oraz ich zabezpieczeń).	Budynek chroniony kartami Secure Identity Object, hasła do komputerów zmieniane co 30 dni, szafy z dokumentami zamykane na klucz.

V. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

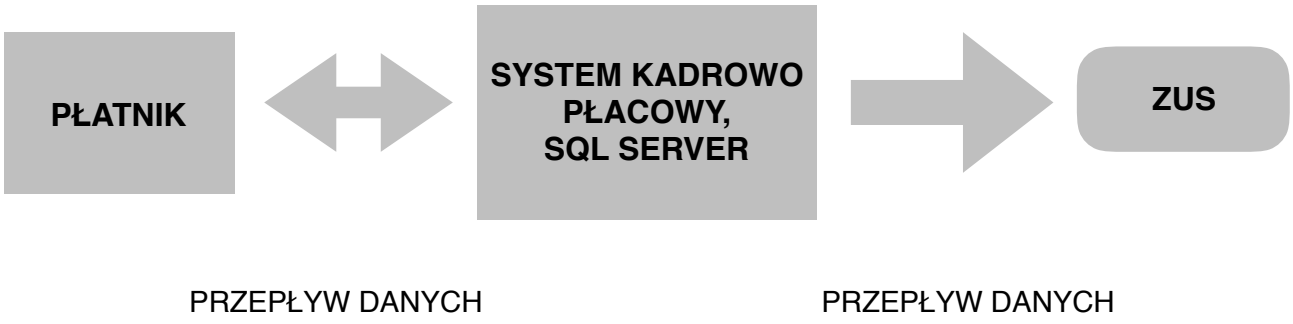
§ 14

PoorSnap, budynek D1 przy ul. Plac Grunwaldzki 13, 50-377

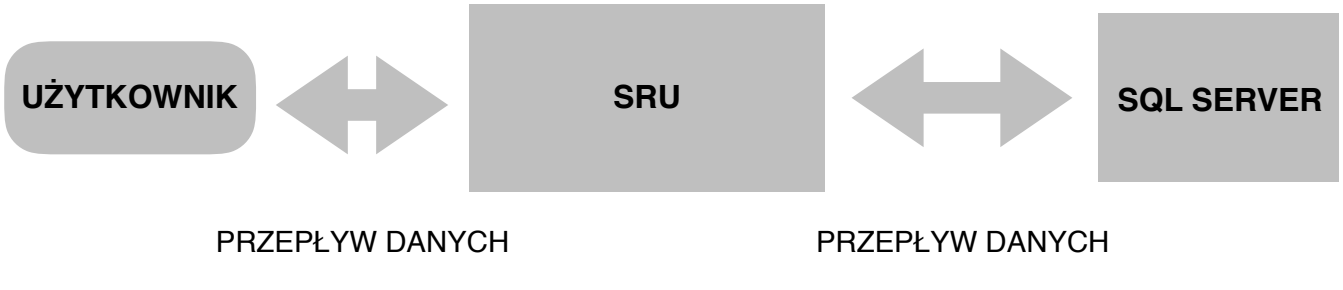
Lp	Zbiór Danych	Dział	Program	Lokalizacja bazy danych	Miejsce przetwarzania danych
1	Dane klientów	Dział reklamacji, dział handlowy	MS SQL Management Studio, MS Office, SRU	Serwer, Archiwum, Jednostki robocze	Pomieszczenia biura, Archiwum w sali 017 budynku D1, serwerownia w 317.2 w budynku D1.
2	Dane kadrowe, Dane ubezpieczonych w ZUS,	Dział księgowy	MS Excel, Płatnik, MS SQL Management Studio	Serwer, Jednostki robocze	Serwerownia w 317.2 w budynku D1.

VI. Sposób przepływu danych między poszczególnymi systemami, współpracy systemów informatycznych ze zbiorami danych

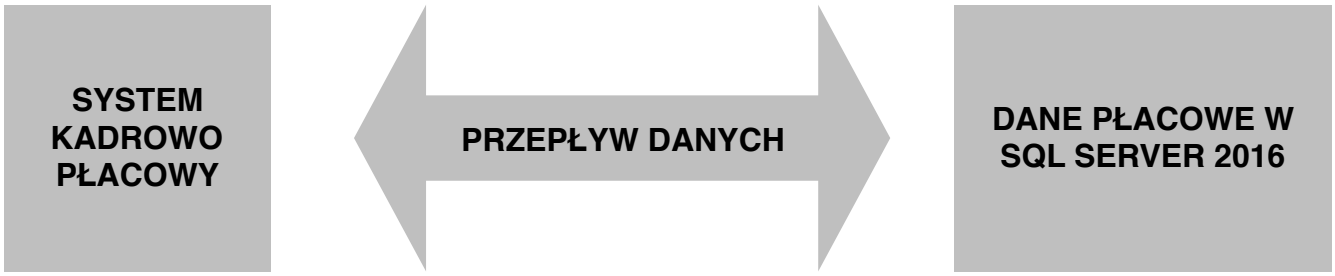
1. Dane ubezpieczeniowe



2. System Reklamacji Użytkownika



3. Kadry i Płace



VII. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych

§ 15

1. Zabezpieczenia organizacyjne:
    1. Sporządzono i wdrożono Politykę Bezpieczeństwa;
    2. Sporządzono i wdrożono instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Krajowej Izbie Doradców Podatkowych;
    3. Wyznaczono ABI
    4. Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora danych bądź osobę przez niego upoważnioną;
    5. Stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;
    6. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
    7. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostany do zachowania ich w tajemnicy;
    8. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
    9. 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;
    10. Dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych.
2. Zabezpieczenia techniczne
    1. Stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową
    2. Komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych za pomocą indywidualnego identyfikatora Active Directory i cyklicznego wymuszania zmiany hasła (Co 30 dni).
3. Środki ochrony fizycznej
    1. Obszar na którym przetwarzane są dane osobowe poza godzinami pracy jest chroniony alarmem,

2. Obszar na którym przetwarzane są dane osobowe objęty jest monitoringiem, oraz jest on dostępny jedynie dla osób posiadających odpowiednią legitymację
3. Urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach

VIII. Instrukcja postępowania w przypadku zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych

§ 16

1. Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.
2. Każdy pracownik bądź członek zarządu **PoorSnap** w przypadku stwierdzenia zagrożenia lub ochrony danych osobowych, zobowiązany jest poinformować Administratora Danych lub ABI
3. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
    1. Niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    2. Niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
    3. Nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.
4. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    1. Zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    2. Zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata lub zagubienie danych).
    3. Umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów lub danych, działanie wirusów i innego szkodliwego oprogramowania).
5. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator Danych lub ABI prowadzi postępowanie wyjaśniające w toku którego:
    1. Ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
    2. Inicjuje ewentualne działania dyscyplinarne,
    3. Rekomenduje działania prewencyjne zmierzające do eliminacji podobnych zagrożeń w przyszłości,
    4. Dokumentuje prowadzone postępowania
6. W przypadku stwierdzenia incydentu, Administrator Danych lub ABI prowadzi postępowanie wyjaśniające w toku, którego:
    1. Ustala czas wystąpienia naruszenia, zakres, przyczyny, skutki, wielkość szkód które zaistniały,
    2. Zabezpiecza ewentualne dowody
    3. Ustala osoby odpowiedzialne za naruszenie,
    4. Podejmuje działania naprawcze,
    5. Inicjuje działania dyscyplinarne
    6. Wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
    7. Dokumentuje prowadzone postępowania.

IX. Zadania Administratora Danych lub Administratora Bezpieczeństwa Informacji

§ 17

Do najważniejszych obowiązków Administratora Danych lub Administratora Bezpieczeństwa Informacji należy:

1. Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
2. Zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki,
3. Wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
4. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
5. Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych, 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

§ 18

Administrator Bezpieczeństwa Informacji ma prawo:

1. wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w **PoorSnap**;
2. wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą;
3. żądania złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;
4. żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;
5. żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

X. Zadania Administratora Systemu Informatycznego

§ 19

1. Administrator Systemu Informatycznego odpowiedzialny jest za:
    1. Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych.
    2. Optymalizację wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego.
    3. Instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego.
    4. Konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym 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 lub Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do informacji w danym systemie.
11. Wnioskowanie do Administratora danych lub Administratora Bezpieczeństwa Informacji w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń.
12. Zarządzanie licencjami, procedurami ich dotyczącymi.
13. Prowadzenie profilaktyki antywirusowej.

2. Praca Administratora Systemu Informatycznego jest nadzorowana pod względem przestrzegania ustawy o ochronie danych osobowych, 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 oraz Polityki Bezpieczeństwa przez Administratora danych lub Administratora Bezpieczeństwa Informacji.

XI. Sprawozdanie roczne stanu systemu ochrony danych osobowych

§ 20

1. Corocznie do dnia **4 kwietnia** ABI lub wyznaczony przez Administratora danych pracownik przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych,
2. W spotkaniu sprawozdawczym uczestniczą: Administrator danych oraz ABI. Na wniosek co najmniej jednego z uczestników w spotkaniu mogą wziąć udział: członkowie zarządu, informatyk, kierownicy działów/jednostek.
3. Sprawozdanie przygotowywane jest w formie pisemnej.

XII. Szkolenia użytkowników

§ 21

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 lub ABI.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora danych, a także o zobowiązaniu się do ich przestrzegania.
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.

5. Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

XIII. Postanowienia końcowe

§ 22

1. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
2. Administrator danych lub Administrator Bezpieczeństwa Informacji ma obowiązek zapoznać z treścią Polityki każdego użytkownika.
3. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
5. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
6. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
7. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.