ZARZĄDZENIE NR 5
WÓJTA GMINY ŚWIĄTKI
z dnia 27 stycznia 2016 roku

w sprawie przyjęcia Polityki Bezpieczeństwa Informacji, Instrukcji Zarządzania Systemem Informatycznym, w którym przetwarzane są dane osobowe oraz powołania Administratora Bezpieczeństwa Informacji i Administratora Systemów Informatycznych w Urzędzie Gminy w Świątkach.

Na podstawie art. 33 ust. 3 Ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (t.j. Dz.U. z 2015 roku, poz. 1515), art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz.U. z 2015 roku, poz. 2135), § 3 ust. 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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 roku, nr 100, poz. 1024) oraz §44 Regulaminu Organizacyjnego Urzędu Gminy w Świątkach zarządzam, co następuje:

§ 1

1. Wprowadzam do użytku służbowego w Urzędzie Gminy w Świątkach:
   1) „Politykę Bezpieczeństwa Informacji", stanowiącą załącznik nr 1 do Zarządzenia.
   2) „Instrukcję Zarządzania Systemem Informatycznym, w którym przetwarzane są dane osobowe", stanowiącą załącznik nr 2 do Zarządzenia.

§ 2

1. Wyznaczam Sekretarza Gminy na Administratora Bezpieczeństwa Informacji w Urzędzie Gminy w Świątkach.
2. Wyznaczam informatyka na Administratora Systemów Informatycznych w Urzędzie Gminy w Świątkach.

§ 3

1. Zobowiązuje się Sekretarza Gminy do zapoznania pracowników Urzędu Gminy w Świątkach z treścią Zarządzenia.
2. Zobowiązuje się pracowników Urzędu Gminy w Świątkach do stosowania i przestrzegania dokumentów określonych w § 1 zarządzenia.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1
do Zarządzenia Nr 5
Wójta Gminy Świątki
z dnia 27 stycznia 2016 roku

POLITYKA
BEZPIECZEŃSTWA INFORMACJI

w Urzędzie Gminy w Świątkach

Świątki
gmina, w której warto żyć

Świątki, styczeń 2016 rok

Spis treści:

§ 1
Wprowadzenie

1. Polityka Bezpieczeństwa Informacji w dalszej części dokumentu zwana Polityką opracowana została w oparciu o następujące przepisy prawa:
   1) Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r., poz. 2135)
   2) Ustawę z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U z 2010 r. Nr 182, poz. 1228 z późn. zm.)
   3) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 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. 2004 nr 100, poz. 1024).
2. Polityka określa zbiór zasad przetwarzania danych osobowych w Urzędzie Gminy w Świątkach oraz ich zabezpieczania, jako zestaw praw, reguł i zaleceń, regulujących sposób ich zarządzania, ochrony i dystrybucji w UG w Świątkach.
3. Celem Polityki jest wdrożenie i realizacja działań przy wykorzystaniu środków technicznych i organizacyjnych, które zapewnią maksymalny poziom bezpieczeństwa w zakresie przetwarzania danych osobowych, chroniąc je przed nieautoryzowanym dostępem, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.
4. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:
   1) poufności – właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom,
   2) integralności – właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   3) rozliczalności – właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
   4) zgodności z prawem – właściwości zapewniającej, że gromadzone są wyłącznie dane niezbędne do właściwego funkcjonowania przedsiębiorstwa.
5. Polityka zakłada pełne zaangażowanie kierownictwa oraz wszystkich pracowników UG w Świątkach dla zapewnienia bezpieczeństwa danych osobowych przetwarzanych zarówno w sposób tradycyjny papierowy, jak i w systemach informatycznych czy innych nośnikach danych.
6. Niniejsza Polityka oraz dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawa oraz w związku ze zmianami, które powodują, że określone zasady przestają być aktualne.

§ 2
Definicje

1. **Administrator Danych Osobowych** – osoba decydująca o celach i środkach przetwarzania danych osobowych – Wójt.
2. **Administrator Bezpieczeństwa Informacji** – osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.
3. **Administrator Systemów Informatycznych** – osoba wyznaczona przez Administratora Danych Osobowych odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych w systemach informatycznych stosowanych w UG w Świątkach, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu informatycznego, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.
4. **Dane osobowe** – każda informacja dotycząca osoby fizycznej, która w sposób pośredni lub bezpośredni pozwala ją zidentyfikować, w szczególności poprzez podanie jednego lub kilku specyficznych czynników ją określających.
5. **GIODO** – Generalny Inspektor Ochrony Danych Osobowych.
6. **Naruszenie ochrony danych osobowych** – zamierzone lub przypadkowe działanie lub zaniechanie działania, powodujące zagrożenie bezpieczeństwa danych osobowych, przetwarzanych tradycyjnie, jak również z wykorzystaniem systemów informatycznych.
7. **Osoba upoważniona** – osoba posiadająca imienne upoważnienie wydane przez Administratora Danych Osobowych lub Administratora Bezpieczeństwa Informacji i dopuszczona jako użytkownik do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu.
8. **Osoba trzecia** – należy przez to rozumieć, osobę nie będącą pracownikiem i współpracownikiem UG w Świątkach, dla której nie istnieją podstawy prawne do nadania jej upoważnienia do przetwarzania danych osobowych.
9. **Przetwarzanie danych osobowych** – 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.
10. **Poufność** – właściwość zapewniająca, że informacja (np. dane osobowe) jest dostępna jedynie osobom upoważnionym.

11. **Rozliczalność**– właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
12. **Ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 roku, poz. 2135).
13. **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 roku, nr 100, poz. 1024).
14. **System informatyczny** – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
15. **Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
16. **Właściciel zasobów** – osoba odpowiedzialna za gromadzenie i przetwarzanie danych osobowych w komórce organizacyjnej.
17. **Zbiór nieinformatyczny** – zbiór danych osobowych prowadzony poza systemem informatycznym, w szczególności w postaci papierowej.

§ 3
Deklaracja Administratora Danych Osobowych

1. Administrator danych zobowiązuje się do podjęcia odpowiednich kroków mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności dane osobowe są:
   1) przetwarzane zgodnie z prawem,
   2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnie z tymi celami,
   3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   4) zabezpieczone środkami technicznymi i organizacyjnymi, które zapewniają rozliczalność, integralność i poufność tych danych.

§ 4
Przegląd dokumentacji ochrony danych osobowych.

1. Niniejsza polityka oraz dokumenty z nią powiązane winny być aktualizowane wraz ze zmianami prawnymi czy też zmianami faktycznymi w ramach przedsiębiorstwa,

które mogą spowodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne.

2. Zadaniem przeglądu jest stwierdzenie, czy postanowienia normowane Polityką odpowiadają aktualnej działalności przedsiębiorstwa oraz stanowi prawnemu w momencie dokonywania przeglądu.
3. Fakt wystąpienia naruszeń winien skutkować zmianami Polityki i dokumentacji powiązanej.
4. Wszelkie zmiany Polityki – mające wpływ na poziom bezpieczeństwa ochrony danych osobowych – winny być zatwierdzane przez Administratora Danych Osobowych.

§ 5

Zarządzanie obszarem ochrony danych osobowych

1. Realizację zadań mających na celu zwiększenie skuteczności ochrony danych osobowych powinny zagwarantować następujące założenia:
   1) przeszkolenie pracowników dopuszczonych do przetwarzania danych w zakresie bezpieczeństwa danych osobowych.
   2) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację w systemach informatycznych (np. hasła, identyfikatory), umożliwiających im dostęp do danych osobowych – stosownie do zakresu upoważnienia i indywidualnych poziomów uprawnień.
   3) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych.
   4) podejmowanie niezbędnych działań, w celu likwidacji słabych ogniw w systemie ochrony danych osobowych.
   5) śledzenie osiągnięć w dziedzinie bezpieczeństwa fizycznego, bezpieczeństwa systemów informatycznych i – w miarę możliwości organizacyjnych i techniczno – finansowych
   6) wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania, służących wzmocnieniu bezpieczeństwa przetwarzanych danych osobowych.
2. Na każdym etapie przetwarzania danych osobowych należy brać pod uwagę, w niezbędnym zakresie, integralność, poufność oraz rozliczalność dla przetwarzanych danych osobowych.
3. Administrator Danych Osobowych powinien mieć pewność, że pracownicy oraz współpracownicy:
   1) są odpowiednio wprowadzani w swoje obowiązki i odpowiedzialności związane z ochroną danych osobowych i ich przetwarzaniem przed przyznaniem im dostępu do danych osobowych;
   2) otrzymali zalecenia określające wymagania w zakresie bezpieczeństwa danych osobowych związane z ich obowiązkami służbowymi;

3) wypełniali zalecenia i warunki zatrudnienia, które uwzględniają zasady ochrony danych osobowych oraz właściwe metody pracy;
4) w sposób ciągły utrzymywali odpowiednie umiejętności i kwalifikacje.

4. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba, przetwarzająca te dane w zakresie zgodnym z zakresem upoważnienia, kompetencjami i rolą sprawowaną w procesie.

§ 6

Odpowiedzialność Administratora danych osobowych

1. Administrator Danych Osobowych jest odpowiedzialny za przetwarzanie danych osobowych oraz za ich ochronę zgodnie z przepisami prawa. W tym celu zobowiązany jest do wprowadzenia do stosowania procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych, rozumiane jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.
2. Do kompetencji Administratora Danych Osobowych należy w szczególności:
   1) wyznaczenie ABI oraz ASI;
   2) wskazanie Właścicieli zasobów danych osobowych;
   3) określenie celów i procedur ochrony danych osobowych;
   4) podział zadań i obowiązków związanych z organizacją obszaru ochrony danych osobowych.
3. Do obowiązków Administratora Danych Osobowych należy:
   1) zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych;
   2) zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem;
   3) przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych;
   4) nadawanie pracownikom upoważnień do przetwarzania danych osobowych;
   5) zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, w których przetwarzane są dane osobowe oraz środków niezbędnych do zapewnienia możliwie najwyższego poziomu bezpieczeństwa danych przetwarzanych w systemach informatycznych;
   6) zapewnienie realizacji obowiązku zgłoszenia i aktualizacji zbiorów danych osobowych do rejestracji GIODO.

§ 7

Odpowiedzialność Administratora Bezpieczeństwa Informacji

1. Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.
2. Do kompetencji Administratora Bezpieczeństwa Informacji należy:
   1) określenie zasad ochrony danych osobowych.
   2) wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony danych osobowych.
3. Do obowiązków Administratora Bezpieczeństwa Informacji należy:
   1) nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych;
   2) nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych;
   3) zapoznawanie pracowników oraz współpracowników z przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem;
   4) reprezentowanie Administratora Danych w kontaktach z Biurem GIODO;
   5) prowadzenie rejestru zbiorów danych osobowych;
   6) reagowanie na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dotyczących ukarania winnych naruszeń
   7) sprawdzanie wypełnienia obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych;
   8) prowadzenie pełnej dokumentacji związanej z ochroną danych osobowych, zawierającej:
      a) ewidencję zbiorów danych osobowych,
      b) ewidencje osób upoważnionych do przetwarzania danych osobowych,
      c) rejestr zbioru danych osobowych,
      d) dokumenty z audytów i przeglądów bezpieczeństwa,
      e) oryginały i kopie dokumentów dotyczących ochrony danych osobowych, w szczególności uchwały, dokumenty dot. polityki bezpieczeństwa, instrukcje, regulaminy, procedury,
      f) programy szkoleń, listę przeszkolonych osób,
      g) kopie wniosków o rejestrację zbiorów,
      h) raport z wypełnienia obowiązku informacyjnego (kopie wniosków, pism z klauzulami informacyjnymi).

§ 8

Odpowiedzialność Administratora Systemów Informatycznych

1. Funkcję Administratora Systemów Informatycznych pełni pracownik wyznaczony przez Administratora Danych Osobowych.
2. Do obowiązków Administratora Systemów Informatycznych należy:
   1) zabezpieczenie systemów przetwarzania danych osobowych;
   2) nadzór oraz zapewnianie ciągłości działania systemu informatycznego;
   3) nadzór nad działaniem i aktualizacja programów antywirusowych zainstalowanych w systemach informatycznych;
   4) reagowanie na przypadki naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych;
   5) przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych;
   6) zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z Ustawą oraz z niniejszą Polityką bezpieczeństwa i Instrukcją Zarządzania Systemem Informatycznym;
   7) instalację oraz konfigurację oprogramowania, sprzętu sieciowego i serwerowego używanego do przetwarzania danych osobowych;
   8) konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem;
   9) nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania;
   10) nadzór nad systemem komunikacji w sieci komputerowej;
   11) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
   12) przyznawanie na wniosek Właściciela zasobów, za zgodą Administratora Danych, ściśle określonych praw dostępu do danych osobowych w danym systemie;
   13) świadczenie pomocy technicznej w ramach oprogramowania a także serwis sprzętu komputerowego będącego na stanie przedsiębiorstwa, służącego do przetwarzania danych osobowych;
   14) diagnozowanie i usuwanie awarii sprzętu komputerowego;
   15) wykonywanie i zarządzanie kopiami zapasowymi oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie) i sieciowego;
   16) nadzór nad wdrożeniem i zarządzanie systemami Informatycznymi (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, itp.), w których przetwarza się dane osobowe;

17) umożliwienie przeprowadzenia kontroli systemu informatycznego przez służby Biura Generalnego Inspektora Ochrony Danych Osobowych.

§ 9
Odpowiedzialność Właścicieli Zasobów

1. Do kompetencji Właścicieli zasobów danych osobowych należy:
   1) określenie celów w jakich mają być przetwarzane dane osobowe, zakresu oraz sposobu ich przetwarzania danych osobowych;
   2) ustalenie, czy dane przetwarzane dla określonego celu mają mieć charakter poufny.
2. Do obowiązków Właścicieli zasobów danych osobowych należy:
   1) zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia;
   2) zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu;
   3) realizację obowiązku informowania o przetwarzaniu danych osobowych osób, których dane osobowe są pozyskiwane;
   4) zapewnienie na żądanie uprawnionych osób, udostępniania informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione.

§ 10
Odpowiedzialność pracowników i użytkowników systemu.

1. W celu zapewnienia wysokiego poziomu bezpieczeństwa danych osobowych konieczne jest zaangażowanie każdego pracownika w proces ochrony danych osobowych.
2. Pracownicy odpowiedzialni są za bezpieczeństwo danych, do których mają dostęp zgodnie z przyznanymi upoważnieniami.
3. Do obowiązków pracowników należy:
   1) informowanie o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach Ustawy;
   2) postępowania zgodnie z przyjętą Polityką;
   3) zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia;
   4) ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;

5) ścisłego przestrzegania zakresu nadanego upoważnienia do przetwarzania danych osobowych;
6) przestrzeganie procedur związanych z otwieraniem i zamykaniem pomieszczeń, w których przetwarzane są dane osobowe a także z wejściem do tych obszarów osób nieupoważnionych;
7) każdorazowe zamykanie systemów informatycznych oraz wyłączanie komputerów i drukarek po zakończeniu pracy;
8) informowanie Administratora Danych lub Administratora Bezpieczeństwa Informacji o podejrzanych osobach.

§ 11

Sankcje prawne za naruszenie zasad ochrony danych osobowych.

W przypadku naruszenia przepisów lub zasad postępowania, osoba upoważniona do przetwarzania danych osobowych podlega odpowiedzialności służbowej i karnej. Naruszenie zasad ochrony danych osobowych a także sposobu ich zabezpieczania, może skutkować postawieniem pracownikowi zarzutu popełnienia, jednego z przestępstw określonych w Rozdziale 8 Ustawy lub przestępstwa określonego w art 266 Kodeksu Karnego.

§ 12

Wymiana informacji dotyczących danych osobowych.

1. W celu ochrony danych pracownicy podczas przetwarzania danych osobowych winni uwzględniać następujące zasady:
   1) wykorzystywać techniki kryptograficzne do ochrony poufności, integralności i rozliczalności danych osobowych przesyłanych publicznymi sieciami telekomunikacyjnymi;
   2) chronić dane osobowe przed przechwyceniem, kopiowaniem, modyfikacją lub zniszczeniem;
   3) zabezpieczenia i ograniczenia związane z przekazywaniem wiadomości za pomocą środków komunikacji, np. automatyczne przekazywanie poczty elektronicznej na zewnątrz;
   4) zakaz pozostawiania informacji zawierających dane osobowe przy urządzeniach drukujących, do których mogą mieć dostęp osoby nieupoważnione;
   5) upewnić się, że rozmówcą jest osoba upoważniona do uzyskania określonych danych osobowych;
   6) zachowanie szczególnej ostrożności w trakcie rozmów telefonicznych;

7) nie pozostawianie wiadomości zawierających dane osobowe na automatycznych sekretarkach;
8) właściwe postępowanie z faksami i kopiarkami z uwagi na pamięć podręczną.

§ 13

Identyfikacja obszarów bezpiecznych.

1. Dane osobowe w Urzędzie Gminy w Świątkach mogą być przetwarzane wyłącznie w pomieszczeniach przetwarzania danych osobowych, na które składają się pomieszczenia biurowe zlokalizowane w budynku urzędu.
2. Do pomieszczeń przetwarzania danych osobowych zalicza się:
   1) serwerownię;
   2) pomieszczenia biurowe, w których znajdują się stacje robocze;
   3) pomieszczenia, w których przechowywane są dokumenty czy wydruki z systemu informatycznego;
   4) pomieszczenia, w których znajdują się zbiory nieinformatyczne;
   5) pomieszczenia, w których znajdują się sprawne oraz uszkodzone elektroniczne nośniki informacji oraz kopie zapasowe.
3. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe winny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych w sposób ograniczający możliwość dostępu do nich osobom nieupoważnionym.
4. W celu ograniczenia dostępu osób nieupoważnionych do pomieszczeń, w których przetwarzane są dane osobowe należy:
   1) określić granice obszaru przetwarzania danych osobowych oraz umiejscowienie dostosowane do wymagań bezpieczeństwa w odniesieniu do aktywów znajdujących się wewnątrz obszaru;
   2) określić granice budynków oraz pomieszczeń, w których przetwarzane są dane osobowe- zamykać drzwi i okna w pomieszczeniach pozostawionych bez dozoru oraz rozważyć zastosowanie rozwiązań ochrony zewnętrznej dla okien, szczególnie tych położonych na poziomie gruntu;
   3) stosować system wykrywania włamań zgodnych z normami w strefach bezpieczeństwa.
5. Obszary bezpieczne winny być odpowiednio zabezpieczone przed skutkami pożaru (ochrona p.poż.).
6. Ochrona obszarów bezpiecznych winna być zapewniona poprzez odpowiednie fizyczne zabezpieczenia wejścia zapewniające to, że tylko osoby upoważnione mogą uzyskać dostęp.

W tym celu należy zapewnić:

1) nadzór pobytu osób nie będących pracownikami UG w Świątkach w obszarach bezpiecznych;
2) kontrolę i ograniczenie dostępu do obszarów, w których przetwarzane są dane osobowe tylko dla osób uprawnionych;
3) przegląd praw dostępu do obszarów bezpiecznych.

7. Nośniki elektroniczne zawierające dane osobowe winny być ewidencjonowane i przechowywane w zamykanych szafkach, które znajdują się w obszarach przetwarzania danych osobowych.

§ 14

Środki ochrony danych osobowych

1. Administrator Danych Osobowych zobowiązany jest zapewnić zastosowanie środków technicznych oraz organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych.
2. Środki ochrony obejmują:
   1) środki fizyczne;
   2) środki osobowe;
   3) środki techniczne.
3. Środki ochrony fizycznej obejmują:
   1) zastosowanie elektronicznego systemu monitoringu na terenie UG w Świątkach;
   2) nadzorowanie pobytu osób nie będących pracownikami przedsiębiorstwa w obszarach bezpiecznych;
   3) lokalizację miejsc przetwarzania danych osobowych;
   4) przechowywanie zbiorów danych osobowych w odpowiednio zabezpieczonych pomieszczeniach;
   5) wdrożenie procedur pobierania kluczy do pomieszczeń.
4. Środki ochrony osobowej obejmują:
   1) dopuszczenie do danych osobowych wyłącznie osób posiadających imienne upoważnienie do przetwarzania danych osobowych wydane przez Administratora Danych Osobowych;
   2) przeszkolenie pracowników z zakresu ochrony danych osobowych;
   3) odebranie stosownych oświadczeń o zachowaniu w poufności danych osobowych.
5. Środki ochrony technicznej obejmują:
   1) mechanizmy i procedury kontroli dostępu do systemów i zasobów;
   2) informatyczne narzędzia ochronne;

3) procedury tworzenia kopii zapasowych;
4) ewidencja przenośnych nośników informacji;
5) procedury postępowania z przenośnymi komputerami, dyskami i nośnikami informacji.

§ 15

Zasady ochrony zbiorów nieinformatycznych.

1. Zbiory nieinformatyczne winny być odpowiednio zabezpieczone przed nieuprawnionym dostępem i zniszczeniem.
2. Dokumenty i wydruki zawierające dane osobowe należy przechowywane w zamykanych pomieszczeniach, do których dostęp mają jedynie uprawnione osoby.
3. Na czas nieużytkowania dokumenty i wydruki zawierające dane osobowe winny być zamykane w szafkach biurowych lub zamykanych szufladach.
4. Wydruki robocze, błędne lub zdezaktualizowane winny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.

§ 16

Dopuszczenie do przetwarzania danych osobowych / ewidencja osób upoważnionych.

1. Pracownicy i współpracownicy mają prawo do przetwarzania danych osobowych wyłącznie po uzyskaniu formalnego upoważnienia do przetwarzania danych osobowych, wystawionego przez Administratora Danych Osobowych.
2. W tym celu Administrator Danych Osobowych / Administrator Bezpieczeństwa Informacji przed dopuszczeniem pracownika do pracy przy przetwarzaniu danych osobowych:
   1) zapoznaje pracownika z przepisami dotyczącymi ochrony danych osobowych oraz uregulowaniami wewnętrznymi obowiązującymi w przedsiębiorstwie;
   2) wystawia pracownikowi formalne upoważnienie do przetwarzania danych osobowych, zgodnie ze wzorem upoważnienia stanowiącym załącznik nr 1 do niniejszej Polityki;
   3) przyjmuje od pracownika podpisane oświadczenie o zachowaniu w poufności danych osobowych i sposobów ich zabezpieczenia, zgodnie ze wzorem oświadczenia stanowiącym załącznik nr 2 do niniejszej Polityki;
   4) upoważnienia i oświadczenia, o którym mowa powyżej przechowuje się w aktach osobowych pracownika.
3. Osoby upoważnione do przetwarzania danych osobowych powinny być wpisywane do ewidencji. Ewidencja osób upoważnionych do przetwarzana danych osobowych powinna być prowadzona przez Administratora Bezpieczeństwa Informacji i powinna zawierać:

1) imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych;
2) zakres upoważnienia do przetwarzania danych osobowych;
3) wskazanie komórki organizacyjnej, w której osoba upoważniona pracuje;
4) identyfikator, jeśli osoba upoważniona została zarejestrowana w systemie informatycznym, służącym do przetwarzania danych osobowych;
5) datę nadania i odebrania uprawnień.

4. Ewidencja osób upoważnionych do przetwarzania danych osobowych winna być przechowywana w szafie zamykanej, do której dostęp ma Administrator Bezpieczeństwa Informacji.
5. Wzór karty z ewidencji osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 3 do niniejszej Polityki.

§ 17

Rejestracja zbiorów danych osobowych / wykaz zbiorów.

1. Kierownik komórki organizacyjnej UG w Świątkach odpowiedzialny jest zgłosić Administratorowi Bezpieczeństwa Informacji zamiar utworzenia nowego zbioru danych osobowych wraz z wskazaniem podstawy przetwarzania danych, uzasadnieniem celowości, zakresu i sposobu zbierania danych osobowych.
2. Administratora Bezpieczeństwa Informacji weryfikuje wniosek o utworzenie nowego zbioru danych osobowych oraz analizuje nowy zbiór danych pod kątem obowiązku ujęcia w prowadzonym Rejestrze.
3. Administrator Bezpieczeństwa Informacji wspólnie z wnioskodawcą określa warunki techniczne i organizacyjne dotyczące zabezpieczeń w systemie informatycznym, a w przypadku niewystarczającego poziomu zabezpieczeń występuje z wnioskiem do Administratora Danych o podniesienie poziomu tych zabezpieczeń.
4. Administrator Bezpieczeństwa Informacji - po akceptacji Administratora Danych Osobowych - rejestruje wniosek.
5. Administrator Bezpieczeństwa Informacji uzupełnia Politykę, dokumenty z nią powiązane oraz pozostałe dokumenty obowiązujące w przedsiębiorstwie w zakresie ochrony danych osobowych o informacje na temat nowego zbioru.

§ 18

Opis struktury zbiorów danych osobowych.

1. Dane osobowe mogą być przetwarzane w zbiorach danych, przy zastosowaniu systemów informatycznych oraz zbiorów ewidencyjnych w postaci kartotek, skorowidzów, wydruków, ksiąg i wykazów.

2. Zawartość pól informacyjnych występujących w systemach zastosowanych w celu przetwarzania danych osobowych, musi być zgodna z przepisami prawa, które uprawniają lub zobowiązują Administratora Bezpieczeństwa Informacji do przetwarzania danych osobowych.
3. Administrator Systemów Informatycznych w oparciu o informacje uzyskane od Właścicieli zasobów danych osobowych, prowadzi - Ewidencję stosowanych systemów i programów (w tym licencji oprogramowania), zastosowanych do przetwarzania danych osobowych.
4. Opis struktury zbiorów danych osobowych przetwarzanych w systemach informatycznych prowadzi Administrator Systemów Informatycznych.
5. Na żądanie Administrator Bezpieczeństwa Informacji lub osoby przez niego upoważnionej, Administrator Systemu Informatycznego zobowiązany jest do wskazania powiązań między polami informacyjnymi, które zawierają dane osobowe w systemie.
6. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.
7. Przepływ jednokierunkowy oznacza, że system informatyczny udostępnia dane ze zbioru (bazy) danych tylko w trybie „do odczytu".
8. Przepływ dwukierunkowy umożliwia upoważnionemu użytkownikowi korzystanie z danych w trybach „do odczytu" i „do zapisu", tj. umożliwia wprowadzanie nowych danych i modyfikację istniejących.
9. Przesyłanie danych pomiędzy systemami może odbywać się w sposób manualny, przy wykorzystaniu nośników zewnętrznych (np. płyta CD, DVD, dysk wymienny, PenDrive itp.) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu/ importu danych za pomocą teletransmisji (np. poprzez szyfrowaną sieć teleinformatyczną).

§ 19

Udostępnienie danych osobowych.

1. Dane osobowe mogą być udostępniane podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Udostępnianie danych osobowych osobie nieupoważnionej do przetwarzania danych osobowych, może nastąpić wyłącznie za zgodą Właściciela zasobów danych osobowych. Zgoda może dotyczyć również udostępniania danych osobowych w przyszłości. Zarówno wniosek jak i zgoda powinny być wystosowane z zachowaniem formy pisemnej.
3. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

4. Na pisemny wniosek pochodzący od osoby, której dane dotyczą, informacje o osobie powinny być udzielone w terminie 30 dni od daty złożenia wniosku.
5. Za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku jest odpowiedzialny Właściciel zasobów danych osobowych.
6. Odpowiedź na wniosek o udostępnienie danych osobowych przed wysłaniem jest akceptowana i parafowana przez Właściciela zasobów danych osobowych oraz Administratora Bezpieczeństwa Informacji a następnie podpisywana przez Administratora Danych.
7. W przypadku odpowiedzi na wniosek, o którym mowa w ust. 2, nie od osoby, której dane dotyczą, Właściciel zasobów danych osobowych przekazuje kopię odpowiedzi do Administratora Bezpieczeństwa Informacji.

§20

Powierzanie danych osobowych.

1. Powierzenie przetwarzania danych osobowych występuje wówczas, gdy podmioty zewnętrzne współpracujące z przedsiębiorstwem mają dostęp do danych osobowych przetwarzanych w przedsiębiorstwie.
2. Powierzenie może mieć miejsce wyłącznie w trybie przewidzianym zapisami art. 31 Ustawy poprzez podpisanie stosownej pisemnej umowy powierzenia pomiędzy Administratorem Danych a podmiotem, któremu powierzono przetwarzanie danych osobowych.

§ 21

Postępowanie w przypadku naruszenia ochrony danych osobowych

W przypadku naruszenia przepisów lub zasad postępowania, osoba upoważniona do przetwarzania danych osobowych podlega odpowiedzialności służbowej i karnej. Naruszenie zasad ochrony danych osobowych a także sposobu ich zabezpieczania, może skutkować postawieniem pracownikowi zarzutu popełnienia, jednego z przestępstw określonych w Rozdziale 8 Ustawy lub przestępstwa określonego w art 266 Kodeksu Karnego

§ 22

Postanowienia końcowe

1. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą która dopuściła się naruszenia.

2. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2002 r., Nr 101, poz. 926 ze zm.) oraz przepisy wykonawcze do tej Ustawy.

Załączniki:

- załącznik nr 1 – Upoważnienie do przetwarzania danych osobowych;
- załącznik nr 2 – Oświadczenie pracownika;
- załącznik nr 3 – Ewidencja osób upoważnionych do przetwarzania danych osobowych;

Załącznik nr 1

UPOWAŻNIENIE NR …../.....
DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity: t.j. Dz.U. z 2015 roku, poz. 2135) upoważniam:

Panią/a ….....

zatrudnioną na stanowisku …..... w Urzędzie Gminy w Świątkach do dostępu do następujących danych osobowych:

a) …..
b) …..

2. Okres trwania upoważnienia: od dnia …..... r. do dnia …..... r.
3. Upoważnienie traci moc w momencie cofnięcia, upływu terminu nadania upoważnienia lub ustania stosunku pracy.
4. Jest Pan/Pani* upoważniony/upoważniona* do przetwarzania danych osobowych wyłącznie w celu wynikającym z Pana/Pani* zadań służbowych oraz poleceń przełożonego.
5. Jednocześnie zobowiązuję Pana/Panią do przestrzegania przepisów dotyczących ochrony danych osobowych zawartych w cytowanej wyżej ustawie z dnia 29 sierpnia 1997 r.

Świątki, dn. …..... r.

Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej:

Załącznik nr 2

Oświadczenie – wzór

Oświadczam, że zostałam/em przeszkolona/y, zapoznałam/em się i będę przestrzegać obowiązków związanych z ochroną danych osobowych, które wynikającą z przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, aktów wykonawczych wydanych na jej podstawie oraz dokumentów przyjętych przez ……. w związku z przetwarzaniem danych osobowych, a w szczególności:

1. Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Świątkach.
2. Instrukcji zarządzania systemem informatyczny w Urzędzie Gminy w Świątkach.

Zobowiązuję się do podejmowania działań zmierzających do zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem.

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskam dostęp w trakcie zatrudnienia, jak również po ustaniu zatrudnienia.

Jednocześnie jestem świadom odpowiedzialności za niedopełnienie obowiązków wynikających z przepisów prawa, jaka ciąży na mnie na podstawie przepisów Regulaminu pracy, Kodeksu pracy oraz Ustawy o ochronie danych osobowych.

.....

Imię i nazwisko pracownika

.....

(podpis Administratora Danych)

Potwierdzam odbiór 1 egz. oświadczenia:

.....

(data i podpis pracownika)

Załącznik nr 3

Wykaz

osób upoważnionych do przetwarzania danych osobowych zatrudnionych w Urzędzie Gminy w Świątkach

Lp.	Imię i Nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Identyfikator[1]	Numer wydanego upoważnienia
1				–		
2.						
3				–		
4				–		
5.				–		
6.				–		
7.				–		
8.				–		
9.				–		
10.				–		
11.				–		
12.						
13.						
14.						
15.						

1 Jeżeli dane są przetwarzane w systemie informatycznym

Załącznik nr 2
do Zarządzenia Nr 5
Wójta Gminy Świątki
z dnia 27 stycznia 2016 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

w Urzędzie Gminy w Świątkach

Świątki
gmina, w której warto żyć

Świątki, styczeń 2016 rok

Spis treści:

§1
Wprowadzenie

1. Instrukcja zarządzania systemem informatycznym w Urzędzie Gminy w Świątkach, zwana w treści niniejszego dokumentu „Instrukcją" określa zasady postępowania, jakie muszą być stosowane przez osoby przetwarzające dane osobowe w systemach informatycznych.
2. Instrukcja została opracowana w oparciu o unormowania zawarte w § 5 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 roku, nr 100, poz. 1024).
3. Podstawowym celem zabezpieczeń systemów informatycznych jest zapewnienie, jak najwyższego poziomu bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych oraz zagwarantowanie zgromadzonym danym charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności.

§ 2
Szkolenia z zakresu ochrony danych osobowych

1. Użytkownicy systemów informatycznych podlegają systematycznym szkoleniom stosownie do potrzeb wynikających ze zmian w systemie informatycznym oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą regulacji wewnętrznych.
2. Za organizację i przeprowadzenie szkoleń z zakresu:
   1) zmian w przepisach dot. ochrony danych osobowych odpowiedzialny jest Administrator Bezpieczeństwa Informacji;
   2) zmian w systemie informatycznym odpowiedzialny jest Administrator Systemów Informatycznych.

§ 3

Obowiązki Administratora Systemów Informatycznych (ASI)

1. Do obowiązków Administratora Systemów Informatycznych w zakresie ochrony danych osobowych przetwarzanych w tych systemach należy w szczególności:
   1) realizacja zadań określonych w § 8 i § 18 Polityki Bezpieczeństwa Informacji;
   2) zarządzanie systemami informatycznymi w sposób zapewniających ochronę danych osobowych;
   3) przestrzeganie opracowanych dla systemów procedur operacyjnych i bezpieczeństwa;
   4) nadzór nad przepływem informacji pomiędzy systemami informatycznymi a siecią publiczną oraz nadzór nad działaniami inicjowanymi z sieci publicznej, a systemami informatycznymi;
   5) zarządzanie środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmian na podstawie zaakceptowanych wniosków przez osobę do tego upoważnioną;
   6) sporządzanie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe kontrole poprawności wykonania kopii zapasowych;
   7) wykonywanie lub nadzór nad wykonaniem okresowych przeglądów i konserwacji sprzętu infrastruktury informatycznej, systemów informatycznych, aplikacji oraz nośników informacji, na których zapisane są dane osobowe.

§ 4

Obowiązki użytkowników

1. Do obowiązków Właścicieli zasobów danych osobowych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:
   1) zapewnienie, we współpracy z Administratorem Systemów Informatycznych, właściwego poziomu ochrony danych osobowych w systemach, dla danych osobowych, za które Właściciele są odpowiedzialni;
   2) informowanie Administratora Bezpieczeństwa Informacji, o zmianie celu przetwarzania danych w systemie lub poszerzeniu zakresu zbieranych danych osobowych;
   3) udostępnianie danych osobowych wyłącznie osobom upoważnionym lub uprawnionych do ich uzyskania.

2. Do obowiązków użytkowników systemów informatycznych w zakresie ochrony danych osobowych w systemach informatycznych należy w szczególności:
   1) przestrzeganie opracowanych dla systemów informatycznych zasad przetwarzania danych osobowych;
   2) przestrzeganie opracowanych dla systemu procedur operacyjnych i procedur bezpieczeństwa;
   3) uniemożliwienie dostępu lub podglądu danych osobowych w systemie dla osób nieupoważnionych;
   4) wykonywanie poleceń Administratora Bezpieczeństwa Informacji w zakresie ochrony danych osobowych, jeśli są one zgodne z przepisami prawa.

§ 5

Eksploatacja systemów informatycznych

1. Zabronione jest:
   1) wprowadzanie zmian do oprogramowania, sprzętu poprzez samodzielne konfigurowanie i wyposażanie;
   2) instalowania nowego oprogramowania lub aktualizacji już zainstalowanego oprogramowania;
   3) korzystania z systemów informatycznych dla celów innych niż te związane z wykonywaniem zadań służbowych;
   4) korzystania z prywatnego sprzętu, w tym oprogramowania oraz nośników pamięci;
   5) umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych;
   6) podejmowania prób testowania, modyfikowania oraz naruszania zabezpieczeń danych lub jakichkolwiek działań noszących takie znamiona;
   7) kopiowania plików zawierających dane osobowe z serwerów na stacje robocze użytkowników i na nośniki informacji, chyba że zgodę na takie działania wyrazi Administrator Bezpieczeństwa Informacji.
2. Informacje przetwarzane przy użyciu aplikacji sieciowych na stacjach roboczych muszą być zapisywane na dyskach serwera.
3. Wszystkie aplikacje sieciowe muszą być ulokowane na przeznaczonych do tego celu serwerach.

§ 6

Nadawanie uprawnień do przetwarzania danych osobowych

1. Przed przystąpieniem do przetwarzania danych w systemach użytkownicy zobowiązani są do zapoznania się z przepisami i zasadami przetwarzania danych osobowych.
2. Przed dopuszczeniem użytkownika do obsługi systemu powinien on odbyć szkolenie w zakresie obsługi sprzętu informatycznego, oprogramowania oraz aplikacji, która wykorzystywana będzie do realizacji zadań służbowych.
3. Pierwsze zarejestrowanie użytkownika w systemie i nadanie odpowiednich uprawnień do systemu, w którym przetwarzane są dane osobowe musi być poprzedzone złożeniem przez użytkownika oświadczenia o zachowaniu w poufności danych osobowych i sposobu ich zabezpieczenia oraz uzyskania formalnego upoważnienia do przetwarzania danych osobowych.
4. Po spełnieniu wymagań określonych w pkt. 3 następuje nadanie uprawnień do systemów informatycznych.
5. Identyfikator oraz zakres dostępu użytkownika powinien być rejestrowany w ewidencji osób upoważnionych do przetwarzania danych osobowych.
6. Tymczasowe hasło dostępu przekazywane jest użytkownikowi w zamkniętej kopercie.
7. Procedurę nadania uprawnień do przetwarzania danych osobowych należy stosować odpowiednio w przypadku zmiany lub odebrania uprawnień.
8. Rozwiązanie umowy o pracę, umowy o współpracę lub utrata upoważnienia są przesłanką do natychmiastowego wyrejestrowania użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych oraz unieważnienia hasła i odnotowania tego faktu w ewidencji osób upoważnionych do przetwarzania danych osobowych.
9. Dostęp do systemu informatycznego czy do poszczególnych aplikacji i baz danych winien być możliwy tylko po podaniu identyfikatora odrębnego dla każdego użytkownika i poufnego hasła.

§ 7

Metody i środki uwierzytelniania w systemie

1. Identyfikatory i hasła są gwarantem rozliczalności, poufności i integralności danych osobowych, które przetwarzane są w systemach informatycznych. Służą m.in. do

weryfikacji tożsamości użytkownika, uzyskania dostępu do określonych zasobów.

2. Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa użytkownicy systemu powinni stosować się do następujących zasad:
   1) użytkownik posiada unikalny identyfikator do swojego osobistego i wyłącznego użytku;
   2) hasło dostępu do systemów informatycznych powinno być utworzone przez użytkownika i stanowić tajemnicę służbową;
   3) użytkownik ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie;
   4) hasło nie może być ujawnione lub przekazane komukolwiek;
   5) użytkownik nie powinien przechowywać hasła w widocznych miejscach.
3. Użytkownicy odpowiedzialni są za wszelkie działania w systemach informatycznych, które prowadzone są z użyciem ich identyfikatora i hasła.
4. Administrator Systemów Informatycznych jest odpowiedzialny za okresowe sprawdzanie systemu pod kątem występowania w nim nieaktywnych kont użytkowników.

§ 8

Wymogi dotyczące uwierzytelniania

1. Wszystkie konta dostępowe do systemów informatycznych winny być chronione hasłem lub innym bezpiecznym sposobem uwierzytelniania.
2. Identyfikator oraz nadane uprawnienia winny umożliwiać wykonywanie czynności wyłącznie zgodnych z zakresem powierzonych obowiązków.
3. Identyfikator użytkownika winien być niepowtarzalny. Po wyrejestrowaniu z systemu informatycznego lub utracie ważności identyfikator nie może być przydzielony innej osobie.
4. Hasło początkowe służy do jednorazowego zarejestrowania użytkownika w systemie i winno być natychmiast zmienione.
5. Hasło składa się z długości minimum 8 znaków i zawierać litery, cyfry i znaki specjalne.
6. Hasła nie mogą być zapisywane w systemach w postaci jawnej i powinny być utrzymane w tajemnicy również po upływie ich ważności.
7. Należy unikać ponownego używania starych haseł.
8. Użytkownicy posiadający wysokie uprawnienia nie powinni wykorzystywać swojego konta do przetwarzania danych osobowych w systemie. Jeśli zachodzi potrzeba

przetwarzania danych osobowych przez użytkownika o wysokich uprawnieniach, dla tego użytkownika powinno zostać założone odrębne konto, które nie jest związane z wysokimi uprawnieniami.

9. Udostępnienie hasła osobie postronnej traktowane jest jako incydent naruszenia ochronny danych osobowych.

§ 9
Wymogi dotyczące zmiany haseł

1. Użytkownik zobowiązany jest do zmiany hasła nie rzadziej niż raz w miesiącu oraz w przypadku ujawnienia lub podejrzenia ujawnienia hasła.
2. W przypadku braku dostępu do konta chronionego hasłem, w którego posiadaniu się znajduje, użytkownik zobowiązany jest wystąpić o zmianę hasła do Administratora Systemów Informatycznych w sytuacji:
   1) zapomnienia lub zagubienia hasła;
   2) wygaśnięcia ważności hasła;
   3) zablokowania konta w wyniku nieprawidłowego wprowadzenia hasła.

§ 10
Procedura bezpiecznego uwierzytelniania

1. Procedura bezpiecznego uwierzytelniania zapewnia minimalizację ryzyka wystąpienia nieautoryzowanego dostępu do systemu. W celu ujawnienia informacji / dodatkowych wskazówek należy zapewnić:
   1) wyświetlenie ostrzeżenia o dostępie jedynie dla uprawnionych użytkowników;
   2) zatwierdzanie jedynie kompletnych informacji wejściowych niezbędnych przy procesie logowania;
   3) ograniczenie liczby nieudanych prób logowania do systemu do najwyżej trzech;
   4) uwzględnić:
      a) wykonanie zapisów nieudanych i udanych prób logowania;
      b) wymuszanie dostępu czasowego przed każdą kolejną próbą logowania;
      c) rozłączanie połączeń;
      d) wysyłanie informacji alarmowej na konsolę systemową w przypadku, gdy maksymalna liczba prób została osiągnięta;
      e) ograniczenie maksymalnego i minimalnego czasu trwania logowania.

2. Wyświetlanie następujących informacji po pomyślnym zalogowaniu:
   1) datę i czas ostatniego pomyślnego logowania do systemu;
   2) szczegółowe dane dotyczące nieudanych prób logowania się, jakie zdarzyły się od chwili ostatniej udanej próby,
3. Blokowanie wyświetlania hasła w trakcie wprowadzania lub ukrywanie wprowadzanych znaków pod symbolami.
4. Blokowanie przesyłania niezaszyfrowanych haseł przez sieć.

§ 11

Wymagania w zakresie sprzętu i oprogramowania

1. Wygaszacz stacji roboczej aktywuje się automatycznie po upływie 10 minut od ostatniego użycia stacji roboczej uruchamiając blokadę, która wymusza ponowne uwierzytelnienie.
2. Dane osobowe winny uniemożliwiać osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora.
3. Oprogramowanie musi być użytkowane z zachowaniem praw autorskich i posiadać licencje.
4. Przed instalacją nowego oprogramowania Administrator Systemów Informatycznych zobowiązany jest sprawdzić jego działanie pod katem bezpieczeństwa całego systemu.
5. Sieć teleinformatyczna wykorzystywana do przetwarzania danych osobowych winna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu informatycznego.
6. Serwer winien być zasilany przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie zasilania przez co najmniej 20 minut oraz na wykonanie bezpiecznego wyłączenia serwera, tak aby przed zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na danych osobowych.
7. Pomieszczenia serwerowni oraz pomieszczenia, w których przetwarzane są dane osobowe winny być odpowiednio chronione przed skutkami pożaru.
8. Infrastruktura techniczna związana z siecią teleinformatyczną i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.
9. Gniazda zasilania sieci teleinformatycznej powinny być odpowiednio oznakowane, zabezpieczone przed włączeniem do nich innych odbiorników i wykonane w specjalnym standardzie.

10. Należy przechowywać wszystkie poprzednie wersje oprogramowania jako środek utrzymania ciągłości działania.
11. Należy zapewnić rejestrowanie wszystkich błędów, związanych z problemami przetwarzania danych osobowych, zgłaszanych przez użytkowników lub programy systemowe.
12. Należy chronić informacje zawarte w dziennikach zdarzeń systemów przed manipulacja i nieautoryzowanym dostępem.
13. Należy zapewnić synchronizację zegarów wszystkich stosowanych systemów służących do przetwarzania danych osobowych z uzgodnionym, dokładnym źródłem czasu.

§ 12

Funkcjonalność systemu informatycznego

1. System informatyczny służący do przetwarzania danych osobowych, z wyjątkiem systemu służącego wyłącznie do edycji tekstu w celu udostępnienia go na piśmie, powinien zapewniać dla każdej osoby, której dane osobowe są przetwarzane w tym systemie - z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie - automatyczne odnotowywanie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych, informacji o dacie pierwszego wprowadzenia danych do systemu oraz o identyfikatorze osoby wprowadzającej dane.
2. W przypadku zbierania danych osobowych od osoby, której dane nie dotyczą należy zapewnić w systemie informatycznym odnotowywanie informacji o źródle pochodzenia danych. Proces ten nie musi odbywać się automatycznie.
3. Dla każdego systemu służącego do przetwarzania danych osobowych, z którego udostępniane są dane osobowe odbiorcom danych, należy zapewnić odnotowanie w bazie danych tego systemu informacji, komu, kiedy i w jakim zakresie dane zostały udostępnione, chyba, że dane pochodzą z jawnego zbioru danych osobowych.
4. Należy zapewnić dla każdej osoby, której dane osobowe są przetwarzane W systemie informatycznym sporządzenie i wydrukowanie:
   1) zestawień zakresu i treści przetwarzanych na jej temat danych osobowych;
   2) zestawienia zawierającego informacje wymagane w § 7 ust. 1 Rozporządzenia.
5. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach, wymagania, o których mowa w § 7 ust. 1 pkt 4 Rozporządzenia, mogą być realizowane w jednej z nich lub w odrębnej aplikacji przeznaczonej do tego celu.

6. Treść ostatecznego rozstrzygnięcia indywidualnej sprawy osoby, której dane dotyczą, nie może być wyłącznie wynikiem operacji na danych osobowych, prowadzonych w aplikacji lub systemie informatycznym.
7. Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w aplikacjach ewidencjonujących osoby fizyczne.

§ 13

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Przed przystąpieniem do pracy z systemem, użytkownik obowiązany 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, użytkownik systemu zobowiązany jest poinformować o tym fakcie bezpośredniego przełożonego. Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest zablokować swoją stację roboczą.
3. Kończąc pracę, użytkownik obowiązany jest do wylogowania się z systemu informatycznego i zabezpieczenia stanowiska pracy, w szczególności wszelkiej dokumentacji, wydruków oraz wymiennych nośników informacji, na których znajdują się dane osobowe i umieszczenia ich zamykanych szafkach.

§ 14

Przetwarzanie danych osobowych

1. W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność, integralność i rozliczalność tych danych, przez co rozumie się:
   1) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi;
   2) stosowanie metod kryptograficznych;
   3) stosowanie odpowiednich zabezpieczeń fizycznych;
   4) stosowanie odpowiednich zabezpieczeń organizacyjnych.
2. W zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.

3. Kopiowanie przez użytkowników plików z serwerów na stacje robocze użytkowników i na elektroniczne nośniki informacji jest zabronione bez akceptacji ze strony Administratora Bezpieczeństwa Informacji.
4. W przypadku udostępniania danych osobowych odbiorcy danych w rozumieniu art. 7 pkt 6 Ustawy, użytkownik ma obowiązek odnotować komu i kiedy udostępniono poszczególne dane.
5. Jeżeli dane osobowe nie są pozyskane od osoby, której dotyczą, użytkownik zobowiązany jest odnotować w systemie informatycznym źródło pochodzenia danych.
6. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych nie podlegających archiwizacji w odrębnym trybie dla którego cel przetwarzania ustał, Administrator Bezpieczeństwa Informacji lub osoby upoważnione sporządzają protokół, w którym zamieszcza następujące informacje:
   1) datę dokonania likwidacji;
   2) przedmiot likwidacji (aplikacja, baza);
   3) podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.
7. Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w systemach informatycznych podejmują Właściciele zasobów danych osobowych.
8. W przypadku likwidacji elektronicznych nośników informacji, należy dokonać wcześniej skutecznego usunięcia danych z tych nośników. W przypadku gdy usunięcie danych nie jest możliwe, należy uszkodzić nośniki w sposób uniemożliwiający odczyt tych danych na przykład poprzez użycie odpowiedniej niszczarki, urządzenia demagnetyzującego itp.
9. Przed przekazaniem elektronicznego nośnika informacji osobie nieuprawnionej, należy usunąć z nośnika w sposób trwały dane osobowe.

§ 15
Kopie zapasowe

1. Kopie zapasowe zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania powinny być wykonywane - zgodnie z planem archiwizacji - przez Administratora Systemów Informatycznych.
2. Kopie zapasowe powinny być tworzone na nośnikach elektronicznych, odpowiednio opisanych, oznakowanych i ewidencjonowanych a każdy proces wykonywania kopii zapasowej powinien być dokumentowany.

3. Kopie zapasowe należy opisywać w sposób umożliwiający szybką i jednoznaczną identyfikację zawartych w nich danych.
4. W celu usystematyzowania procesu wykonywania kopi zapasowej, odpowiedzialny za ten proces Administrator Systemów Informatycznych, jest zobowiązany do sporządzenia harmonogramu wykonywania kopi zapasowej, wraz z opisem narzędzi służących do jej wykonywania, nazwą polityk, nazwą systemu, nazwą bazy danych, terminem okresu przechowywania, rodzajem wykorzystywanego nośnika wraz z numerem seryjnym nośnika.
5. Tworzenie, przechowywanie i likwidację kopii zapasowych powinny regulować szczegółowe instrukcje operacyjne dla poszczególnych systemów informatycznych, opracowywane przez Administratora Systemów Informatycznych, z uwzględnieniem niniejszych postanowień.
6. Administrator Systemów Informatycznych odpowiedzialny za tworzenie kopi zapasowych, zobowiązany jest przestrzegać terminów sporządzania kopii zapasowych oraz okresowo dokonywać kontroli możliwości odtworzenia danych zapisanych na tych kopiach, pod kątem ewentualnej przydatności w sytuacji awarii systemu.
7. Kopie zapasowe powinny być tworzone w bezpiecznym systemie archiwizacji, który powinien zapewniać ograniczony dostęp fizyczny do nośników oraz przyznanie uprawnień dostępu tylko wyznaczonemu Imiennie Administratorowi Systemów Informatycznych oraz Administratorowi Bezpieczeństwa Informacji.
8. Dane z kopii zapasowych powinny być odtwarzane wyłącznie przez Administratora Systemów Informatycznych oraz upoważnionych przez Administratora Danych pracowników.
9. Kopie zapasowe, które uległy uszkodzeniu powinny podlegać natychmiastowemu zniszczeniu.

§ 16

Przechowywanie nośników elektronicznych zawierających dane osobowe

1. Dane osobowe przechowywane są na serwerach znajdujących się w obszarach bezpiecznych, nośnikach elektronicznych oraz na stacjach roboczych znajdujących się na stanowiskach pracy.
2. Po zakończeniu przetwarzania danych osobowych w postaci elektronicznej należy usunąć dane z nośnika elektronicznego w sposób uniemożliwiający ich ponowne odtworzenie.
3. Używanie wymiennych nośników elektronicznych winno być ściśle nadzorowane.

4. Wymienne nośniki elektroniczne winny być przechowywane w zamykanych szafkach.
5. Nośniki zawierające kopie zapasowe winny być przechowywane w innym pomieszczeniu niż pomieszczenie, w którym znajduje się serwer i przechowywane w ognioodpornej szafie, do której dostęp mają wyłącznie osoby upoważnione.

§ 17

Ochrona przed działaniem szkodliwego oprogramowania

1. Na stacjach roboczych oraz na serwerze zainstalowane jest oprogramowanie antywirusowe skanujące na bieżąco system informatyczny.
2. Oprogramowanie antywirusowe zainstalowane jest tak, aby użytkownik nie był w stanie wyłączyć go lub pominąć etapu skanowania.
3. Kontrola antywirusowa przeprowadzana jest na wszystkich nośnikach magnetycznych i optycznych służących zarówno do przetwarzania danych osobowych w systemie jak i do celów instalacyjnych.
4. Należy stosować wersje programów antywirusowych z aktualną bazą sygnatur wirusów.
5. Nowe wersje oprogramowania antywirusowego oraz uaktualnienia bazy sygnatur wirusów instaluje Administrator Systemów Informatycznych niezwłocznie po ich otrzymaniu lub ściągnięciu, uprzednio weryfikując pochodzenie oprogramowania.
6. W przypadku zainfekowania systemu Administrator Systemów Informatycznych jest odpowiedzialny za usunięcie wirusa.
7. Administrator Systemów Informatycznych ma prawo odłączyć stację roboczą, na której zlokalizowany został wirus, jeśli uzna, że dalsze pozostawienie do w sieci zagraża innym stacjom roboczym.

§ 18

Przeglądy i konserwacje systemu informatycznego

1. Przeglądy, naprawy i konserwacje systemu informatycznego dokonywane na miejscy jego użytkowania dokonywane są w obecności Administratora Systemów Informatycznych.
2. Za prawidłowość przeprowadzenia przeglądów oraz dokumentowanie zmian w systemie odpowiada Administrator Systemów Informatycznych.
3. W przypadku konieczności dokonania 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 umowę powierzenia danych osobowych, zgodnie z unormowaniami zawartymi w art. 31 Ustawy.

4. Przegląd oprogramowania winien być przeprowadzony w przypadku zmiany wersji oprogramowania aplikacji, bazy danych lub wykonania zmian w systemie spowodowanych koniecznością naprawy lub konserwacji.
5. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych.
6. Każda zmian parametrów systemu winna być dokładnie dokumentowana.
7. Raz w roku należy przeprowadzać weryfikację całego oprogramowania użytkowego eksploatowanego na wszystkich stacjach roboczych podłączonych do systemu informatycznego pod kątem spełnienia wymogów bezpieczeństwa.

§ 19
Procedury postępowania z komputerami przenośnymi

1. Użytkownik komputera przenośnego zawierającego dane osobowe jest zobowiązany zachować szczególną ostrożność przy transporcie, przechowywaniu i użytkowaniu poza obszarem przetwarzania danych osobowych.
2. Użytkownik komputera przenośnego zawierającego dane osobowe powinien:
   1) stosować środki ochrony kryptograficznej wobec danych osobowych przetwarzanych na tym komputerze;
   2) zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego – identyfikator i hasło;
   3) chronić dostęp do komputera przed osobami nieupoważnionymi;
   4) nie wykorzystywać komputera w obszarach użyteczności publicznej;
   5) zachować szczególną ostrożność przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych.
3. W przypadku komputera przenośnego do sieci publicznej poza siecią przedsiębiorstwa należy zastosować firewall zainstalowany bezpośrednio na tym komputerze oraz program antywirusowy.
4. Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego użytkownik.

§ 20

Postanowienia końcowe

W sprawach nieuregulowanych w Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t.j. Dz.U. z 2015 r., poz. 2135) oraz przepisy wykonawcze do Ustawy.