

Zarządzenie Nr 65/2017
Burmistrza Miasta Pionki
z dnia 24 kwietnia 2017 r.

**w sprawie: wdrożenia dokumentacji bezpieczeństwa informacji i ochrony danych osobowych
w Urzędzie Miasta Pionki**

Na podstawie art. 31 oraz art. 33 ustawy z dnia 8 marca o samorządzie gminnym (tj. Dz. U. z 2016 r. poz. 446 z późn. zm.), w związku z art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2016 r. poz. 922) oraz § 3 rozporządzenia Ministra spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)

Zarządzam, co następuje:

§ 1

1. Wprowadzam do stosowania „**Politykę bezpieczeństwa informacji w Urzędzie Miasta Pionki**”, w brzmieniu stanowiącym załącznik nr 1 do niniejszego zarządzenia.
2. Wprowadzam do stosowania „**Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Pionki**”, w brzmieniu stanowiącym załącznik nr 2 do niniejszego zarządzenia.

§ 2

1. Wykonanie zarządzenia powierza się Kierownikom komórek organizacyjnych, Administratorowi Bezpieczeństwa Informacji oraz Administratorowi Systemów Informatycznych Urzędu Miasta Pionki, każdemu w swoim zakresie.
2. Zobowiązuję Kierowników komórek organizacyjnych Urzędu Miasta Pionki do zapoznania podległych im pracowników z niniejszą dokumentacją bezpieczeństwa informacji, w szczególności w zakresie ochrony danych osobowych.
3. Nadzór nad wykonaniem zarządzenia powierzam Sekretarzowi Miasta Pionki.

§ 3

Traci moc zarządzenie nr 8/2011 Burmistrza Miasta Pionki z dnia 7 lutego 2011 r. w sprawie: wdrożenia dokumentacji przetwarzania danych osobowych w Urzędzie Miasta Pionki.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ

Romuald Zawodnik

**POLITYKA BEZPIECZEŃSTWA
INFORMACJI
W URZĘDZIE MIASTA PIONKI**

§ 1 Postanowienia ogólne

1. Polityka bezpieczeństwa informacji w Urzędzie Miasta Pionki, zwana dalej „**Polityką**”, została wydana w oparciu normę PN-ISO/IEC 27002, w związku z § 3 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).
2. Celem Polityki jest stworzenie podstaw dla właściwego wykonania obowiązków Administratora Danych w zakresie zabezpieczenia i prawidłowej ochrony przetwarzanych informacji, w szczególności danych osobowych.
3. Polityka określa zasady przetwarzania informacji oraz ich zabezpieczania, jako zestaw praw, reguł i zaleceń, regulujących sposób ich zarządzania, ochrony i dystrybucji wewnątrz Urzędu Miasta Pionki.
4. Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania informacji oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych, zapewniających ochronę przetwarzanych informacji.
5. Niniejszą Politykę stosuje się do:
 - 1) danych osobowych:
 - a) przetwarzanych w systemach informatycznych,
 - b) zapisanych się na zewnętrznych nośnikach informacji,
 - c) przetwarzanych tradycyjnie,
 - 2) pozostałych informacji i dóbr materialnych i niematerialnych, które posiadają wartość dla Urzędu Miasta Pionki, zapewniające jego funkcjonowanie,
 - 3) informacji dotyczących bezpieczeństwa przetwarzania danych:
 - a) służących do uwierzytelnienia w systemach informatycznych, w których są przetwarzane dane osobowe;
 - b) dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.
6. Bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy, zasady określone w niniejszej Polityce oraz w dokumentach powiązanych powinny być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez współpracowników przetwarzających informacje i dane osobowe, których administratorem jest Gmina Miasta Pionki.

§ 2 Definicje

Użyte w niniejszej Polityce pojęcia są wspólne dla „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Pionki” oraz wszystkich dokumentów powiązanych z niniejszą Polityką. Ilekroć w Polityce jest mowa o:

- 1) **ustawie**. – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2016 r. poz. 922 z późn. zm.);
- 2) **rozporządzeniu** – rozumie się przez to 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 2004r. Nr 100, poz. 1024);
- 3) **Generalny Inspektor** – rozumie się przez to Generalnego Inspektora Ochrony Danych Osobowych;
- 4) **Urządzie** – rozumie się przez to Urząd Miasta Pionki;
- 5) **Administratorze Danych** – rozumie się przez to Gminę Miasta Pionki, która decyduje o środkach i celach przetwarzania danych osobowych, reprezentowaną przez Burmistrza Miasta Pionki;
- 6) **ABI** – rozumie się przez to administratora bezpieczeństwa informacji wyznaczonego przez Administratora Danych, odpowiedzialnego za nadzorowanie przestrzegania zasad i wymagań

w zakresie ochrony danych osobowych, wynikających z obowiązujących przepisów o ochronie danych osobowych;

- 7) **ASI** – rozumie się przez to administratora systemów informatycznych wyznaczonego przez Administratora Danych, odpowiedzialnego za funkcjonowanie infrastruktury informatycznej na którą składa się cały sprzęt informatyczny oraz systemy i aplikacje informatyczne, za ich przeglądy, konserwację oraz za stosowanie technicznych i organizacyjnych środków bezpieczeństwa w systemach informatycznych.
- 8) **pracownika** – rozumie się przez to osobę zatrudnioną w Urzędzie, upoważnioną przez Administratora Danych do przetwarzania danych osobowych w Urzędzie, w zakresie wskazanym w upoważnieniu;
- 9) **współpracownika** – należy przez to rozumieć osobę nie będącą pracownikiem, dla której istnieją podstawy prawne, do nadania jej upoważnienia do przetwarzania danych osobowych;
- 10) **właściciela zasobów** – należy przez to rozumieć osobę kierującą komórką organizacyjną Urzędu, odpowiedzialną za ochronę informacji, w szczególności danych osobowych przetwarzanych w podległej komórce;
- 11) **danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników ją określających;
- 12) **zasobie** – rozumie się przez to dobra materialne i niematerialne, które posiadają wartość dla Urzędu Miasta Pionki, zapewniające funkcjonowanie Urzędu np. mienie Urzędu, informacje przetwarzane w Urzędzie, wizerunek Urzędu i inne;
- 13) **integralności danych** – rozumie się przez to właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- 14) **poufności danych** – rozumie się przez to właściwość zapewniającą, że informacja jest dostępna jedynie osobom upoważnionym;
- 15) **rozliczalności** – rozumie się przez to właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
- 16) **naruszeniu ochrony danych osobowych** – rozumie się przez to zamierzone lub przypadkowe działanie lub zaniechanie działania, powodujące zagrożenie bezpieczeństwa danych osobowych, przetwarzanych tradycyjnie, jak również z wykorzystaniem systemów informatycznych;
- 17) **przetwarzaniu danych osobowych** – rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
- 18) **systemie informatycznym** – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
- 19) **identyfikatorze użytkownika (LOGIN)** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- 20) **hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- 21) **zbiorze danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie;
- 22) **zbiorze nieinformatycznym** – każdy zbiór danych osobowych prowadzony poza systemem informatycznym, w szczególności w postaci papierowej - kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego;

§ 3
Obszary ryzyka.
Deklaracja Administratora Danych

1. Zasoby istotne dla realizacji zadań Urzędu, a w szczególności informacje i sprzęt niezbędny do ich przechowywania i przetwarzania, są narażone na różne zagrożenia, które identyfikuje się w następujących obszarach ryzyka:
 - 1) naruszenie poufności - rozumiane jako udostępnienie informacji i zasobów, osobom nieupoważnionym np.: przekazanie informacji pracownikom nieupoważnionym, osobom niezatrudnionym w Urzędzie, kradzież zasobu, zagubienie zasobu;
 - 2) naruszenie dostępności - rozumiane jako, znaczne obniżenie istotnych parametrów funkcjonalnych zasobów lub utrata danych np.: zniszczenie zasobu, kradzież zasobu na skutek wystąpienia sił wyższych albo nieumyślnego, umyślnego lub przypadkowego działania;
 - 3) naruszenie integralności - rozumiane jako, nieautoryzowana zmiana treści informacji na skutek nieumyślnego, umyślnego lub przypadkowego działania;
 - 4) naruszenie autentyczności - rozumiane jako, uniemożliwienie weryfikacji informacji lub danych je opisujących;
 - 5) naruszenie niezaprzeczalności - rozumiane jako, zanegowanie swego uczestnictwa w procesie wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;
 - 6) naruszenie rozliczalności - rozumiane jako, uniemożliwienie weryfikacji działań przez osoby biorące udział w procesach wytwarzania i przetwarzania informacji.
2. Zadaniem regulacji zawartych w Polityce jest zmniejszenie ryzyka płynącego z zagrożeń do akceptowalnego poziomu, to znaczy zminimalizowanie możliwości naruszenia bezpieczeństwa zasobów informacyjnych Urzędu, umożliwienie wczesnego wykrycia takiego naruszenia, zminimalizowanie strat związanych z takim naruszeniem oraz sprawne usunięcie jego skutków
3. Administrator Danych zobowiązuje się do podjęcia odpowiednich kroków, mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności do zapewnienia, że przez cały okres ich przetwarzania, dane będą:
 - 1) przetwarzane zgodnie z prawem;
 - 2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;
 - 3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
 - 4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;
 - 5) zabezpieczone środkami technicznymi i organizacyjnymi, które zapewniają rozliczalność, integralność oraz poufność danych.
4. Przy przetwarzaniu danych osobowych w systemach informatycznych Urzędu Miasta Pionki - należy stosować wysoki poziom bezpieczeństwa w rozumieniu § 6 ust. 4 rozporządzenia.

§ 4
Przegląd dokumentacji z zakresu ochrony danych osobowych

1. Niniejsza Polityka oraz dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach Urzędu, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.
2. Przegląd Polityki ma na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Urzędu oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.
3. Fakty wystąpienia poważnych naruszeń ochrony danych osobowych powinny skutkować zmianami w dokumencie niniejszej Polityki i dokumentach powiązanych.
4. Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów obowiązujących w Urzędzie, dotyczących ochrony danych osobowych.

5. Wszelkie zmiany Polityki – mające wpływ na poziom ochrony danych osobowych - powinny być zatwierdzane przez Administratora Danych.

§ 5

Zarządzanie ochroną danych osobowych

1. W celu zwiększenia skuteczności ochrony danych osobowych należy 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 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 - 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. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba, przetwarzająca te dane w zakresie zgodnym z zakresem upoważnienia, kompetencjami i rolą sprawowaną w procesie przetwarzania danych.

§ 6

Dokumenty powiązane

1. Oryginały i kopie dokumentów dotyczących ochrony danych osobowych (w tym uchwały, zarządzenia, polityki itd.) dotyczące ochrony danych osobowych – prowadzone przez ABI.
2. „Wykaz zbiorów danych osobowych przetwarzanych w Urzędzie, ze wskazaniem programów zastosowanych do ich przetwarzania” (wzór zał. Nr 1 do niniejszej Polityki) – prowadzony przez ABI.
3. „Jawny rejestr zbiorów danych osobowych”, o którym mowa w art. 36a ustawy – prowadzony przez ABI.
4. „Ewidencja osób upoważnionych przez Administratora Danych do przetwarzania danych osobowych” (wzór zał. Nr 2 do niniejszej Polityki) – prowadzona przez ABI
5. Roczne plany sprawdzeń zgodności przetwarzania danych osobowych (wzór zał. Nr 3 do niniejszej Polityki) – prowadzone przez ABI.
6. „Rejestr umów powierzenia przetwarzania danych osobowych”, zawierający: nr i datę zawarcia umowy; podmiot, któremu powierzono przetwarzanie danych osobowych; oznaczenie komórki organizacyjnej i/lub pracownika Urzędu odpowiedzialnych za realizację umowy; czas obowiązywania umowy; zakres przetwarzanych danych osobowych – prowadzony przez ABI.
7. Plan okresowych szkoleń z zakresu ochrony danych osobowych / dokumentacja szkoleniowa – prowadzone przez ABI.
8. „Ewidencja stosowanych systemów i programów” (w tym licencji oprogramowania) – prowadzona przez ASI.
9. Opisy struktur zbiorów danych osobowych wraz z opisami sposobów przepływu danych pomiędzy systemami – prowadzone przez ASI.
10. Plany archiwizacji danych osobowych i programów służących do ich przetwarzania – prowadzone przez ASI.
11. „Rejestr incydentów naruszenia bezpieczeństwa teleinformatycznego” – prowadzony przez ASI.
12. „Ewidencje przenośnych nośników danych używanych w poszczególnych komórkach organizacyjnych” – prowadzone przez właścicieli zasobów.

§ 7

Odpowiedzialność Administratora Danych

1. Administrator Danych jest odpowiedzialny za przetwarzanie i ochronę danych osobowych zgodnie z przepisami prawa, w tym wprowadzenie do stosowania procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych, rozumiane jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabranie przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz utratą, uszkodzeniem lub zniszczeniem.
2. Do kompetencji Administratora Danych należy w szczególności:
 - 1) wyznaczenie Administratora Bezpieczeństwa Informacji;
 - 2) wyznaczenie Administratora/ów Systemów Informatycznych;
 - 3) wyznaczenie Właścicieli zasobów danych osobowych;
 - 4) określenie celów i strategii ochrony danych osobowych;
 - 5) podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.
3. Do obowiązków Administratora Danych 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 zagrożeń związanych z ich przetwarzaniem;
 - 3) przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych w Urzędzie;
 - 4) nadawanie pracownikom i współpracownikom Urzędu upoważnień do przetwarzania danych osobowych (wzór upoważnienia zał. Nr 4 do niniejszej Polityki);
 - 5) zapewnienie środków finansowych niezbędnych do ochrony danych osobowych przetwarzanych w systemach informatycznych oraz w zbiorach nieinformatycznych;
 - 6) zapewnienie środków finansowych na merytoryczne przygotowanie osób odpowiedzialnych za nadzór nad ochroną danych osobowych;
 - 7) zapewnienie prowadzenia i aktualizacji wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
 - 8) zapewnienie prowadzenia i aktualizacji jawnego rejestru zbiorów danych przetwarzanych przez Administratora Danych;
 - 9) zapewnienie zgłoszenia i aktualizacji zbiorów danych osobowych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 i 1a ustawy.

§ 8

Zadania i uprawnienia Administratora Bezpieczeństwa Informacji

1. Administrator Danych może powołać ABI.
2. Do zadań ABI należy zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
 - 1) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora Danych;
 - 2) nadzorowanie opracowania i aktualizacji dokumentacji, o której mowa w art. 36 ust. 2 ustawy, oraz zasad w niej określonych;
 - 3) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
 - 4) zapewnianie złożenia oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania w tajemnicy danych osobowych oraz informacji na temat zabezpieczania danych osobowych przez osoby upoważnione do przetwarzania danych osobowych (wzór oświadczenia zał. Nr 5 do niniejszej Polityki);
 - 5) wydawanie pracownikowi/współpracownikowi, na wniosek Właściciela zbioru danych osobowych, upoważnienia do przetwarzania danych osobowych;

- 6) oświadczenia i upoważnienia, o których mowa w ust. 2 pkt 4 i 5, wystawia się w trzech egzemplarzach, z których 1 egz. otrzymuje pracownik/współpracownik, 1 egz. przechowuje się w aktach osobowych pracownika/współpracownika, 1 egz. pozostaje w aktach spraw prowadzonych przez ABI;
 - 7) zapoznavanie pracowników oraz współpracowników z przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem;
 - 8) prowadzenie ewidencji wydanych upoważnień do przetwarzania danych osobowych;
 - 9) prowadzenie wykazu i rejestru zbiorów danych, o których mowa w § 7 ust. 3, pkt 7 i 8 niniejszej Polityki;
 - 10) przygotowywanie zgłoszenia i aktualizacji zbiorów danych osobowych do rejestracji przez Generalnego Inspektora, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 i 1a ustawy;
 - 11) reprezentowanie Administratora Danych w kontaktach z Generalnym Inspektorem;
 - 12) reagowanie na zgłaszane incydenty (zdarzenia, zajścia lub wypadki nie będące częścią standardowych operacji lub usług, które powodują lub mogą spowodować spadek poziomu ochrony danych osobowych) związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dotyczących ukarania winnych naruszeń;
 - 13) przygotowywanie planów sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania Sprawdzenie wypełnienia obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych.
3. ABI w zakresie realizacji swoich obowiązków, ma prawo: wydawać upoważnienia do przetwarzania danych osobowych, decydować o pozbawieniu lub ograniczeniu zakresu przetwarzanych danych osobowych i uprawnień nadanych w systemach informatycznych dla użytkowników, którzy powodują zagrożenie bezpieczeństwa i ochrony danych osobowych, udzielania wytycznych dotyczących usuwania nieprawidłowości stwierdzonych w czasie prowadzonych sprawdzeń w celu dostosowania ochrony danych osobowych do stanu zgodnego z przepisami, zbierania od użytkowników, ich przełożonych oraz innych osób pisemnych wyjaśnień dotyczących okoliczności powstania zagrożeń dla bezpieczeństwa i ochrony danych osobowych, rozpatrywania skarg i wniosków w zakresie przetwarzania danych osobowych, kontrolowania pracowników w zakresie przestrzegania zasad bezpieczeństwa i ochrony danych osobowych poprzez prowadzone sprawdzenia.

§ 9

Odpowiedzialność Administratora Systemów Informatycznych

1. Rolę ASI pełni pracownik (lub pracownicy) wyznaczony przez Administratora Danych.
2. Do obowiązków ASI należy:
 - 1) zabezpieczenie systemów przetwarzania danych osobowych zgłoszonych ASI, w zależności od kategorii przetwarzanych w tym systemie danych;
 - 2) bieżący nadzór oraz zapewnianie optymalnej ciągłości działania systemu informatycznego w tym opracowanie procedur określających zarządzanie systemem informatycznym przetwarzającym dane osobowe;
 - 3) reagowanie bez zbędnej zwłoki, w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych;
 - 4) przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych;
 - 5) analizę raportów wszelkich zdarzeń w tym incydentów związanych z bezpieczeństwem systemów przetwarzania danych;
 - 6) zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z ustawą oraz z niniejszą Polityką i Instrukcją Zarządzania Systemem Informatycznym w Urzędzie Miasta Pionki;
 - 7) instalację i konfigurację oprogramowania 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 oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji;
- 11) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
- 12) przyznawanie na wniosek właściciela zasobów, zatwierdzanego przez ABI, za zgodą Administratora Danych, ściśle określonych praw dostępu do danych osobowych w danym oprogramowaniu;
- 13) świadczenie pomocy technicznej w ramach oprogramowania a także serwis sprzętu komputerowego będącego na stanie Urzędu, służącego do przetwarzania danych osobowych;
- 14) diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizację umów z firmami świadczącymi usługi pogwarancyjnego sprzętu komputerowego;
- 15) wykonywanie i zarządzanie kopiami zapasowymi oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie);
- 16) prowadzenie dokumentacji, o której mowa w § 6 niniejszej Polityki, § należącej do kompetencji ASI;
- 17) zarządzanie systemami informatycznymi (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, itp.), w których przetwarza się dane osobowe.

§ 10

Odpowiedzialność właścicieli zasobów.

1. Administrator Danych wyznacza właścicieli zasobów, którzy są odpowiedzialni, za ochronę informacji przypisanych i przetwarzanych w podległej komórce organizacyjnej.
2. Do kompetencji właścicieli zasobów w zakresie danych osobowych należy:
 - 1) określanie zgodnych z prawem celów w jakich mają być przetwarzane dane osobowe, zakresu oraz czasu trwania przetwarzania danych osobowych;
 - 2) określenie sposobu przetwarzania danych osobowych (czy w systemach informatycznych, czy w zbiorach nieinformatycznych);
 - 3) ustalenie, czy dane przetwarzane dla określonego celu mają mieć charakter poufny;
 - 4) wnioskowanie do Administratora Danych o nadanie uprawnień do przetwarzania danych przypisanych pracownikom/współpracownikom.
3. Do obowiązków właścicieli zasobów danych osobowych należy:
 - 1) zgłoszenie do ABI nowo utworzonych zbiorów danych osobowych w podległej komórce (wzór zgłoszenia zał. nr 6 do niniejszej Polityki);
 - 2) bezzwłoczne zgłaszanie każdej zmiany informacji zawartej w zgłoszeniu, o którym mowa w pkt 1;
 - 3) jeżeli zmiana informacji, o której mowa pkt. 2, dotyczy rozszerzenia zakresu przetwarzanych danych osobowych, właściciel zasobów jest zobowiązany do jej zgłoszenia przed dokonaniem zmiany w zbiorze;
 - 4) zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w podległej komórce;
 - 5) informowanie o przetwarzaniu danych osobowych osób, których dane osobowe są pozyskiwane;
 - 6) zapewnienie na żądanie uprawnionych osób, udostępnianie informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione;
 - 7) niedopuszczenie do przetwarzania danych osobowych przez pracowników lub współpracowników (o ile to konieczne) bez złożenia oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania w tajemnicy danych osobowych oraz informacji na temat zabezpieczania danych osobowych;
 - 8) prowadzenie ewidencji, o której mowa w § 6 ust. 11 niniejszej Polityki.

§ 11

Odpowiedzialność pracowników i współpracowników

1. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa informacji, w szczególności danych osobowych, konieczne jest zaangażowanie ze strony każdego pracownika i współpracownika w zakresie ochrony informacji.
2. Pracownicy i współpracownicy są zobowiązani do:
 - 1) zgłaszanie wszelkich podejrzeń naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzania danych osobowych bezpośrednio do ABI;
 - 2) postępowania zgodnie z 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.
3. Pracownicy i współpracownicy powinni pamiętać o możliwości zaistnienia ryzyka naruszenia ochrony danych osobowych. W związku z tym powinni:
 - 1) przestrzegać procedury związane z otwieraniem i zamykaniem pomieszczeń, o których mowa w § 14 niniejszej Polityki, a także z przebywaniem w obszarach przetwarzania danych osobowych osób nieupoważnionych;
 - 2) informować bezpośredniego przełożonego o podejrzanych osobach przebywających w obiektach Urzędu,
 - 3) pracownicy/współpracownicy powinni na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać ABI projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu ochrony danych osobowych.

§ 12

Szkolenia w zakresie ochrony danych osobowych

1. Przed rozpoczęciem przetwarzania danych osobowych pracownik powinien odbyć szkolenie wstępne prowadzone przez ABI. Szkolenie wstępne powinno obejmować następujące zagadnienia:
 - 1) wprowadzenie do problematyki ochrony danych osobowych;
 - 2) prawa osób, których dane dotyczą;
 - 3) omówienie przepisów wewnętrznych w zakresie ochrony danych osobowych obowiązujące w Urzędzie;
 - 4) zasady bezpiecznego użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych;
 - 5) zagrożenia na jakie może być narażone przetwarzanie danych osobowych, a w szczególności te związane z przetwarzaniem danych osobowych w systemach informatycznych;
 - 6) zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe;
 - 7) sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego;
 - 8) odpowiedzialność z tytułu naruszenia ochrony danych osobowych.
2. W celu udokumentowania odbycia szkolenia wstępnego, pracownik/współpracownik podpisuje kartę szkolenia (wzór karty, zał. nr 7 do niniejszej Polityki).
3. Szkolenia powinny być powtarzane okresowo lub na żądanie, gdy zaistnieje taka potrzeba.
4. Współpracownicy reprezentujący osoby trzecie (tam, gdzie jest to wskazane) powinni przechodzić przeszkolenie w zakresie wskazanym w ust. 1.

§ 13

Wymiana informacji dotyczących danych osobowych

1. Pracownicy i współpracownicy w celu ochrony wymienianych informacji dotyczących danych osobowych powinni podczas przetwarzania uwzględniać następujące zasady:
 - 1) wykorzystywanie technik kryptograficznych do ochrony poufności, integralności i rozliczalności danych osobowych przesyłanych publicznymi sieciami telekomunikacyjnymi;
 - 2) ochrona wymienianych danych osobowych przed przechwyceniem, kopiowaniem, modyfikacją, błędnym wyborem drogi komunikacji i zniszczeniem;
 - 3) zabezpieczenia i ograniczenia związane z możliwościami przekazywania wiadomości za pomocą środków komunikacji, np. automatyczne przekazywanie poczty elektronicznej na zewnątrz;
 - 4) zakaz pozostawiania informacji zawierających dane osobowe przy urządzeniach drukujących, np. kopiarkach, drukarkach, faksach, do których mogą mieć dostęp osoby nieupoważnione;
 - 5) upewnienie się przed przekazaniem danych osobowych, czy rozmówca jest osobą upoważnioną do uzyskania określonych danych osobowych;
 - 6) zachowania szczególnej ostrożności w trakcie rozmów telefonicznych, unikając podsłuchania danych osobowych przez osoby nieupoważnione;
 - 7) nie pozostawianie wiadomości zawierających dane osobowe w automatycznych sekretarkach;
 - 8) właściwe postępowanie z faksami i fotokopiarkami, ponieważ mają one podręczną pamięć i przechowują w niej strony zawierające np. dane osobowe na wypadek błędów transmisji.
2. Transport danych osobowych w postaci elektronicznej i papierowej pomiędzy obszarami, w których są przetwarzane dane osobowe, powinien być prowadzony przez osoby upoważnione, w sposób ograniczający możliwość ich pozyskania i odczytu przez osoby nieupoważnione.

§ 14

Przetwarzanie danych osobowych w obszarach bezpiecznych

1. Dane osobowe w Urzędzie mogą być przetwarzane wyłącznie w pomieszczeniach przetwarzania danych osobowych.
2. Na pomieszczenia przetwarzania danych osobowych składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie Administrator Danych prowadzi działalność.
3. Do pomieszczeń przetwarzania danych osobowych zalicza się:
 - 1) Serwerownia;
 - 2) pomieszczenia biurowe, w których zlokalizowane są stacje robocze;
 - 3) pomieszczenia, w których przechowywane są sprawne oraz uszkodzone elektroniczne nośniki informacji, kopie zapasowe;
 - 4) pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego;
 - 5) pomieszczenia, w których zlokalizowane są zbiory nieinformatyczne.
4. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe stanowi załącznik nr 8 do niniejszej Polityki.
5. Przebywanie wewnątrz obszarów, o których mowa w ust. 3, osób nieuprawnionych do przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub Właściciela zasobów.
6. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostęp do nich osobom nieupoważnionym.
7. W celu ograniczenia dostępu osób nieupoważnionych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych, należy zapewnić:

- 1) jasne określenie granic obszaru przetwarzania danych osobowych oraz umiejscowienie dostosowane do wymagań bezpieczeństwa w odniesieniu do aktywów znajdujących się wewnątrz obszaru;
 - 2) jednolite granice budynków lub pomieszczeń, gdzie zlokalizowano środki przetwarzania danych osobowych (tzn. aby granice nie miały luk lub punktów, przez które łatwo się włamać);
 - 3) ściany zewnętrzne pomieszczeń solidnej konstrukcji oraz wszystkie drzwi zewnętrzne odpowiednio zabezpieczone przed nieautoryzowanym dostępem za pomocą mechanizmów zabezpieczeń, np. alarmów, zamków itp.;
 - 4) zamykanie drzwi i okien w pomieszczeniach pozostawianych bez dozoru oraz należy rozważyć zastosowanie mechanizmów zewnętrznej ochrony dla okien, szczególnie tych położonych na poziomie gruntu;
 - 5) system wykrywania włamań zgodnych z normami w strefach bezpieczeństwa oraz regularne jego testowanie.
8. Obszary bezpieczne powinny być odpowiednio zabezpieczone przed skutkami pożaru.
 9. Ochrona obszarów bezpiecznych powinna być zapewniona poprzez odpowiednie fizyczne zabezpieczenia wejścia zapewniające, że tylko osoby upoważnione mogą uzyskać dostęp, w tym celu należy zapewnić:
 - 1) nadzorowanie pobytu osób nie będących pracownikami Urzędu w obszarach bezpiecznych, chyba że ich dostęp został wcześniej zaakceptowany;
 - 2) kontrolowanie i ograniczenie dostępu do obszarów, gdzie są przetwarzane dane osobowe tylko dla uprawnionego personelu;
 - 3) regularne przeglądanie praw dostępu do obszarów bezpiecznych i jeśli zachodzi potrzeba, uaktualnianie ich lub odbieranie.
 10. Przetwarzanie danych osobowych jest zakazane w tych pomieszczeniach, w których osoby trzecie wykonują prace techniczne.
 11. Nośniki elektroniczne zawierające dane osobowe powinny być ewidencjonowane i należy przechowywać w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych.
 12. Każdorazowe naruszenie zasad ochrony danych osobowych dane osobowe powinno być zgłaszane ABI.

§ 15

Dopuszczenie osób do przetwarzania danych osobowych

1. Pracownik lub współpracownik mają prawo przetwarzać dane osobowe wyłącznie po uzyskaniu formalnego upoważnienia do ich przetwarzania wydawanego przez ABI. W tym celu właściciel zasobów, przed dopuszczeniem w/w do przetwarzania danych osobowych, wnioskuje do ABI o formalne upoważnienie pracownika/współpracownika do przetwarzania danych osobowych, wskazując: nazwę zbioru (zbiorów), zakres przetwarzania danych w danym zbiorze i okres udzielenia upoważnienia.
2. Właściciele zasobów, przełożeni pracowników i współpracowników odpowiadają za natychmiastowe pisemne zgłoszenie do ABI osób, które utraciły uprawnienia dostępu do danych osobowych.
3. ABI w oparciu o informację, o której mowa w ust. 2 powinien podjąć działania, których celem jest uniemożliwienie tym osobom dostępu do danych osobowych i wyrejestrować je z ewidencji, o której mowa w ust. 1.

§ 16

Ewidencja osób upoważnionych do przetwarzania danych osobowych

1. Osoby upoważnione do przetwarzania danych osobowych powinny być wpisywane do ewidencji osób upoważnionych do przetwarzania danych osobowych, która jest prowadzona przez ABI.
2. Jakakolwiek zmiana w zakresie informacji zawartych w ewidencji powinna podlegać natychmiastowemu odnotowaniu.
3. Elektroniczne nośniki informacji, na których gromadzone są wykazy zawierające ewidencję osób upoważnionych do przetwarzania danych osobowych powinny być przechowywane w szafie zamykanej, do której ma dostęp ABI lub osoba przez niego upoważniona.

§ 17

Dostęp zdalny

1. Zastosowane przez Administratora Danych rozwiązania techniczne umożliwiające dostęp zdalny do danych osobowych powinny zapewniać integralność, poufność i rozliczalność przetwarzanych danych osobowych oraz ochronę kryptograficzną wobec danych służących do uwierzytelnia, a przesyłanych publicznymi łączami telekomunikacyjnymi.
2. Nadawanie uprawnień w celu dostępu zdalnego do systemów informatycznych przetwarzających dane osobowe realizowane jest przez ASI, po spełnieniu wymagań określonych w ust. 1 oraz po uzyskaniu akceptacji Administratora Danych.
3. Dostęp do systemów informatycznych dla współpracowników powinien być monitorowany pod kątem bezpieczeństwa przez ASI w celu zapewnienia poufności, rozliczalności i integralności danych osobowych.

§ 18

Rejestracja i aktualizacja zbiorów danych osobowych

1. Kierownicy komórek organizacyjnych Urzędu są zobowiązani do zgłaszania ABI o zamiarze utworzenia nowego zbioru danych osobowych na formularzu, który stanowi załącznik nr 6 do niniejszej Polityki.
2. ABI weryfikuje wniosek, o którym mowa w ust. 1, pod kątem obowiązku rejestracji zbioru w jawnym rejestrze zbiorów oraz obowiązku zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi.
3. W sytuacji, gdy zbiór wymaga rejestracji przez Generalnego Inspektora, Kierownik komórki zgłaszający zbiór, przygotowuje projekt zgłoszenia wypełniając części A – D zgłoszenia ustalonego na podstawie art. 46a ustawy.
4. Części E – F zgłoszenia, o którym mowa w ust. 3 wypełnia ASI, odpowiedzialny za odpowiednie zabezpieczenie danych w systemie informatycznym Urzędu.
5. ABI sprawdza opisane w zgłoszeniu rejestracyjnym 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.
6. ABI, po akceptacji Administratora Danych, przekazuje wniosek o rejestrację zbioru danych osobowych Generalnemu Inspektorowi.
7. Administrator Danych, na wniosek ABI, wyznacza właściciela zasobów nowo zarejestrowanego zbioru danych osobowych.
8. Obowiązek aktualizacji informacji w zbiorze już zarejestrowanym ciąży na właścicielu danego zbioru. Do zgłaszania zmian stosuje się odpowiednio przepisy o rejestracji zbiorów danych, o których mowa w ust. 1 – 7.

§ 19

Udostępnianie danych osobowych

1. Dane osobowe mogą być udostępniane podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.
2. Udostępnianie danych osobowych osobie nieupoważnionej może podlegać sankcjom określonym w § 26 niniejszej Polityki.
3. Na pisemny wniosek pochodzący od osoby, której dane dotyczą, informacje o osobie powinny być udzielone w terminie 30 dni od daty złożenia wniosku.
4. Za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku jest odpowiedzialny właściciel zasobów.
5. Odpowiedź na wniosek o udostępnienie danych osobowych przed wysłaniem jest akceptowana i parafowana przez właściciela zasobów oraz ABI, a następnie podpisywana przez Administratora Danych.
6. Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom za potwierdzeniem odbioru, np. w następujący sposób:
 - 1) listem poleconym za pokwitowaniem odbioru;

- 2) teletransmisji danych zgodnie z zasadami wymiany informacji opisanymi w § 13 niniejszej Polityki;
- 3) innym bezpiecznym, określonym wymogiem prawnym lub umową.

§ 20

Powierzenie przetwarzania danych osobowych

1. Powierzenie przetwarzania danych osobowych występuje wówczas, gdy podmioty zewnętrzne współpracujące z Urzędem, mają dostęp do danych osobowych przetwarzanych przez Administratora Danych.
2. Wskazane w ust. 1 powierzenie przetwarzania danych osobowych może się odbywać wyłącznie w trybie przewidzianym w art. 31 ustawy poprzez zawarcie na piśmie umowy powierzenia przetwarzania danych osobowych z podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.
3. Nie wymaga zawarcia umowy powierzenie przetwarzania danych, w tym przekazywanie danych, jeżeli ma miejsce między Administratorem Danych, a organami państwowymi, organami samorządu terytorialnego oraz państwowymi i komunalnymi jednostkami organizacyjnymi.
4. W umowie powierzenia przetwarzania danych osobowych określa się w szczególności:
 - 1) cel i zakres przetwarzania danych osobowych;
 - 2) obowiązek podjęcia środków zabezpieczających zbiór danych, o których mowa w art. 36-39 ustawy, oraz spełnienia wymagań określonych w przepisach, o których mowa w art. 39a ustawy;
 - 3) czas trwania umowy, włączając w to przypadki, w których obowiązek zachowania poufności może być bezterminowy.
5. Właściciele zasobów danych osobowych są zobowiązani do przygotowania umowy powierzenia danych osobowych dla zasobów danych osobowych, za które są odpowiedzialni. Umowę, przed podpisaniem przez Administratora Danych, należy przekazać do ABI, w celu oceny jej zgodności z ustawą i niniejszą Polityką.

§ 21

Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Poniższe postanowienia mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych, jak i w zbiorach nieinformatycznych.
2. Przed przystąpieniem do pracy pracownicy/współpracownicy zobowiązani są dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próbę naruszenia ochrony danych osobowych.
3. Za okoliczności, które uznaje się za naruszenie lub podejrzenie naruszenia ochrony systemu przetwarzającego dane osobowe, uważa się w szczególności:
 - 1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują;
 - 2) nieuprawnione naruszenie lub próbę naruszenia poufności, integralności i rozliczalności danych i systemu;
 - 3) niezamierzoną zmianę lub utratę danych zapisanych na kopiach zapasowych;
 - 4) nieuprawniony dostęp do danych osobowych (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu);
 - 5) udostępnienie osobom nieupoważnionym danych osobowych lub ich części;
 - 6) inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy;
 - 7) wydarzenia losowe, obniżające poziom ochrony systemu (np. brak zasilania lub pożar);
 - 8) kradzież sprzętu informatycznego lub nośników zewnętrznych zawierających dane osobowe (np. wydruków komputerowych, dyskietek, płyt CD-ROM, dysków twardych, pamięci zewnętrznych, itp.).

4. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych pracownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie ABI i bezpośredniego przełożonego.
5. Do czasu przybycia ABI, zgłaszający:
 - 1) powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów;
 - 2) zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym;
 - 3) podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych;
 - 4) wykonuje polecenia ABI.
6. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych ABI, po przybyciu na miejsce:
 - 1) ocenia zaistniałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe oraz stan urządzeń, a także szacuje wielkość negatywnych następstw incydentu;
 - 2) wysłuchuje relacji osoby, która dokonała powiadomienia oraz innych osób związanych z incydentem;
 - 3) podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.
7. ABI sporządza raport z przebiegu zdarzenia.
8. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od ABI.
9. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej w Urzędzie dyscypliny pracy, ABI wyjaśnia wszystkie okoliczności incydentu i podejmuje stosowne działania wobec osób, które dopuściły się wskazanego naruszenia.
10. Po zakończeniu czynności naprawczych system powinien utrzymać poziom ochrony nie niższy niż przed wystąpieniem incydentu związanego z naruszeniem ochrony danych osobowych.

§ 22

Wykaz zbiorów danych osobowych

1. ABI prowadzi wykaz zbiorów danych osobowych przetwarzanych przez Administratora Danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, który stanowi integralną część niniejszej Polityki.
2. Oprócz wykazu, o którym mowa w ust. 1, ABI prowadzi jawny rejestr zbiorów danych osobowych przetwarzanych przez Administratora Danych.
3. Każdy ma prawo przeglądać rejestr, o którym mowa w ust. 2.
4. ASI, 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.

§ 23

Opis struktury zbiorów danych osobowych

1. Opis struktury zbiorów danych osobowych przetwarzanych w systemach informatycznych, prowadzi ASI.
2. Zakresy danych osobowych przetwarzanych w poszczególnych zbiorach danych osobowych w systemach informatycznych, są ustalone w oparciu o strukturę zbiorów danych osobowych prowadzonych w tych systemach oraz powiązania pól informacyjnych. ASI wykonuje, na podstawie aplikacji zastosowanych do przetwarzania danych osobowych opisy struktur zbiorów danych wskazujące zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi.
3. Opisy wykonywane są w postaci wydruków zrzutów ekranowych lub struktur tablic bazy prezentujących zawartość pól informacyjnych i powiązań pomiędzy nimi. W przypadku braku możliwości uzyskania wydruku zrzutu ekranowego ASI, sporządza inne dostępne opisy struktury zbioru.

4. ASI zobowiązany jest do prowadzenia i przechowywania opisów struktur zbiorów danych oraz natychmiastowego uaktualniania w przypadku zmian.

§ 24

Sposób przepływu danych pomiędzy poszczególnymi systemami

1. ASI, prowadzi dokumentację systemów informatycznych zawierającą opis współpracy pomiędzy różnymi systemami informatycznymi oraz sposób przepływu danych pomiędzy systemami, w których te dane są przetwarzane.
2. Schematy przepływu danych pomiędzy systemami informatycznymi, zastosowanymi w celu przetwarzania danych osobowych, wykonuje ASI, zgodnie z relacjami występującymi w programach służących do przetwarzania danych osobowych.
3. ASI zobowiązany jest do prowadzenia i przechowywania schematów oraz natychmiastowego ich uaktualniania w przypadku zmian.

§ 25

Zasady ochrony danych osobowych w zbiorach nieinformatycznych

1. Zbiory nieinformatyczne powinny być odpowiednio zabezpieczone przed nieuprawnionym dostępem i zniszczeniem.
2. Dokumenty i wydruki, zawierające dane osobowe, należy przechowywać w zamykanych pomieszczeniach, do których dostęp mają jedynie uprawnione osoby.
3. Na czas nie użytkowania, dokumenty i wydruki zawierające dane osobowe powinny być zamykane w szafach biurowych lub zamykanych szufladach.
4. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanimizowanie.
5. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów archiwalnych, należy stosować odpowiednie przepisy dot. zasad archiwizacji i brakowania dokumentacji Urzędu.

§ 26

Sankcje za naruszenie zasad ochrony danych osobowych

1. Naruszenie zasad ochrony danych osobowych przez pracownika/współpracownika może skutkować postawieniem mu zarzutu popełnienia, jednego z przestępstw określonych w Rozdziale 8 ustawy lub przestępstwa określonego w art. 266 Kodeksu Karnego.
2. Zgodnie z art. 100 § 2 pkt 5 Kodeksu Pracy, pracownik jest obowiązany przestrzegać tajemnicy określonej w odrębnych przepisach. Dane osobowe, którym Urząd Miasta Pionki i nadaje charakter poufny, mają charakter takiej tajemnicy, a jej ujawnienie w zależności od zakresu ujawnionych danych osobowych oraz nastawienia pracownika dopuszczającego się nieuprawnionego ujawnienia danych, może mieć charakter naruszenia lub ciężkiego naruszenia obowiązków pracowniczych.
3. Pracownik dopuszczający się nieuprawnionego ujawnienia lub wykorzystania danych osobowych w sposób sprzeczny z ich przeznaczeniem (np. wykorzystania danych osobowych do celów prywatnych), czy też ich przetwarzania w sposób niezgodny z przyjętymi w Urzędzie procedurami, może zostać ukarany karą upomnienia lub karą nagany.
4. W razie ciężkiego naruszenia obowiązku zachowania danych osobowych w tajemnicy lub przetwarzania ich w sposób rażąco sprzeczny z przyjętymi zasadami i procedurami, Administrator Danych może rozwiązać bez wypowiedzenia umowę o pracę z winy pracownika.
5. Sankcje dotyczące ujawnienia poufnych danych osobowych, stosuje się analogicznie do ujawnienia przez pracownika informacji dotyczących zabezpieczenia danych osobowych w Urzędzie.

§ 27

Postępowanie z informacją

1. Dokumenty stanowiące zasoby informacyjne są oznaczane, przetwarzane, przechowywane i brakowane zgodnie z zapisami rozporządzenia Rady Ministrów z dnia 18 stycznia 2011 r.

w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. z 2011 r. nr 14, poz. 67, ze zm.).

2. Postępowanie z informacjami niejawnymi określa plan ochrony informacji niejawnych Urzędu, określony na podstawie art. 15 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (tj. Dz. U. z 2016 r. poz. 1167, ze zm.) oraz przepisów wykonawczych do tej ustawy.
3. Postępowanie z danymi osobowymi oraz z zasobami informacyjnymi zawartymi na elektronicznych nośnikach danych określają ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i niniejsza Polityka.
4. Zasady postępowania z zasobami (środki trwałe) reguluje ustawa z dnia 29 września 1994 r. o rachunkowości (tj. Dz. U. z 2016 r. poz. 1047, ze zm.).
5. Zasady postępowania z dowodami finansowo-księgowymi reguluje „Instrukcja sporządzania i ewidencji oraz obiegu i kontroli dowodów i dokumentów finansowo- księgowych w Urzędzie Miasta Pionki”.
6. Zasady postępowania z kluczami oraz zabezpieczenia pomieszczeń i budynków, w których są przechowywane i przetwarzane dane osobowe określa „Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń i budynków Urzędu Miasta Pionki”.

§ 28

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 2016 r., poz. 922 z późn. zm.) oraz przepisy wykonawcze do tej ustawy.

Zatwierdził

BURMISTRZ

.....
Romuald Zawodnik

Załącznik Nr 3 – roczny plan sprawdzeń

Lp.	Przedmiot sprawdzenia	Zakres sprawdzenia	Termin sprawdzenia	Sposób i zakres dokumentowania
1.				
2.				

Sporządził:

.....
(data i podpis)

ZATWIERDZAM

.....
(data i podpis)

....., dnia

U P O W A Ż N I E N I E

Nr/.....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

(tj. Dz. U. z 2016 r., poz. 922)

w związku z wnioskiem

z dnia.....

u p o w a ż n i a m

Pana /Panią

.....

do przetwarzania danych osobowych w zbiorze o nazwie :

1.

w zakresie

2.

w zakresie

Niniejsze upoważnienie ma moc obowiązującą od dnia Na czas

Ustanie stosunku pracy powoduje unieważnienie udzielonego upoważnienia.

Niniejsze upoważnienie daje uprawnienia Pana/Pani do dalszych upoważnień w przedmiotowym zakresie.

Jest Pan/Pani* upoważniony/upoważniona* do przetwarzania danych osobowych wyłącznie w zakresie wynikającym z Pana/Pani* zadań służbowych oraz poleceń przełożonego.

Jednocześnie zobowiązuję Pana/Panią do przestrzegania przepisów dotyczących ochrony danych osobowych zawartych w cytowanej wyżej ustawie z dnia 29 sierpnia 1997 r.

.....
(podpis Administratora Danych)

.....
(data i podpis pracownika / współpracownika)

.....
(data)

Oświadczenie

Oświadczam, że zapoznała(e)m się, rozumiem i będę przestrzegać obowiązków wynikających z przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), aktów wykonawczych wydanych na jej podstawie oraz dokumentów przyjętych przez Urząd Miasta Pionki w związku z przetwarzaniem danych osobowych, a w szczególności:

- Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta Pionki;
- Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Pionki.

Zobowiązuję się do podejmowania działań zmierzających do zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem oraz unikaniem tych zachowań, które mogłyby poziom bezpieczeństwa danych osobowych obniżyć.

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

Jednocześnie przyjmuje do wiadomości, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia ponoszę odpowiedzialność na podstawie przepisów Regulaminu pracy, Kodeksu pracy oraz Ustawy o ochronie danych osobowych.

.....
(czytelny podpis pracownika / współpracownika)

.....
(podpis Administratora Danych)

Potwierdzam odbiór 1 egz. oświadczenia:
(data i podpis pracownika / współpracownika)

Załącznik Nr 6 – zgłoszenie zbioru danych osobowych do ABI

Zbiór Nr

(Wypełnia ABI)

Nazwa zbioru danych osobowych			
Oznaczenie administratora danych osobowych	Gmina Miasto Pionki Aleja Jana Pawła II 15 26-670 Pionki REGON 796 295 87 67		
Przedstawiciel administratora danych osobowych, o którym mowa w art. 31a. ustawy o ochronie danych osobowych	nie dotyczy		
Podmioty, którym powierzono przetwarzanie danych ze zbioru			
Podstawa prawna upoważniająca do przetwarzania danych ze zbioru*	Zgoda osoby, której dane dotyczą, na przetwarzanie danych jej dotyczących		
	Przetwarzanie jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa:		
Cel przetwarzania danych w zbiorze	Dopełnienie uprawnień i/lub obowiązków wynikających z ustawy		
Opis kategorii osób, których dane dotyczą			
Zakres danych przetwarzanych w zbiorze*	nazwiska i imiona		Numer Identyfikacji Podatkowej
	imiona rodziców		miejsce pracy
	data urodzenia		zawód
	miejsce urodzenia		wykształcenie
	adres zamieszkania lub pobytu		seria i numer dowodu osobistego
	numer ewid. PESEL		numer telefonu
	Inne dane osobowe, oprócz ww., przetwarzane w zbiorze – podaj jakie:		
Dane wrażliwe, o których mowa w art. 27 ustawy o ochronie danych osobowych*	a) ujawniają bezpośrednio lub w kontekście:		
	pochodzenie rasowe		przynależność partyjną
	pochodzenie etniczne		przynależność związkową
	poglądy polityczne		stan zdrowia
	przekonania religijne		kod genetyczny
	przekonania filozoficzne		nałogi
	przynależność wyznaniową		życie seksualne
	b) dotyczą:		
	skazań		orzeczeń o ukaraniu
	mandatów karnych		innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym
Podstawa prawna przetwarzania danych wrażliwych, o których mowa w art. 27 ustawy o ochronie danych osobowych*	Osoby, których dane dotyczą, będą wyrażać na to zgodę na piśmie,		
	przepis szczególny innej ustawy zezwala na przetwarzanie bez gody osoby, której dane dotyczą, jej danych osobowych – jeżeli TAK, to podaj odniesienie do przepisu tej ustawy:		
	przetwarzanie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,		
	przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem		
Sposób zbierania danych do zbioru*	przetwarzanie jest niezbędne do wykonywania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie		
	od osób, których dotyczą		
Sposób udostępniania danych ze zbioru	z innych źródeł niż osoba, której dane dotyczą		
Informacje o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane			
Informacje dotyczące przekazywania danych do państw trzecich			

Właściciel zbioru danych osobowych

(data i podpis)

* W przypadku odpowiedzi twierdzącej należy zakreślić prostokąt literą "X"

**KARTA Nr
SZKOLENIA WSTĘPNEGO
W ZAKRESIE
OCHRONY DANYCH OSOBOWYCH**

Szkolenie wstępne w zakresie ochrony danych osobowych przeprowadzono zgodnie z § 12 "Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta Pionki" obowiązującej na podstawie zarządzenia nr 8/2011 Burmistrza Miasta Pionki z 7 lutego 2011 r. w sprawie: wdrożenia dokumentacji przetwarzania i ochrony danych osobowych w Urzędzie Miasta Pionki.

Zakres tematyczny szkolenia:

1. Wprowadzenie do problematyki ochrony danych osobowych.
2. Omówienie wybranych przepisów ustawowych obowiązujących w zakresie ochrony danych osobowych.
3. Prawa osób, których dane osobowe dotyczą.
4. Omówienie przepisów wewnętrznych w zakresie ochrony danych osobowych obowiązujących w Urzędzie Miasta Pionki.
5. Zasady bezpiecznego użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych.
6. Zagrożenia na jakie może być narażone przetwarzanie danych osobowych.
7. Zasady zabezpieczenia danych osobowych, w tym dostępu do pomieszczeń, w których przetwarzane są dane osobowe.
8. Sposób postępowania w przypadku naruszenia ochrony danych osobowych.
9. Odpowiedzialność pracownika z tytułu naruszenia ochrony danych osobowych.

Imię i nazwisko osoby odbywającej szkolenie:

Szkolenie przeprowadził:

Data szkolenia:

.....
(podpis szkolącego)

.....
(podpis szkolonego)

Załącznik Nr 8 – Wykaz obiektów tworzących obszar ochrony danych osobowych

**Wykaz
budynków, pomieszczeń lub części pomieszczeń, tworzących obszar,
w którym przetwarzane są dane osobowe**

L. p.	Obszar	Adres

**INSTRUKCJA ZARZĄDZANIA SYSTEMEM
INFORMATYCZNYM SŁUŻĄCYM DO
PRZETWARZANIA DANYCH OSOBOWYCH
W URZĘDZIE MIASTA PIONKI**

§ 1

Postanowienia ogólne

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Pionki, zwana dalej „**Instrukcją**” określa zasady, tryb postępowania i zalecenia Administratora Danych, które muszą być stosowane przez osoby przez niego upoważnione do przetwarzania danych osobowych w systemach informatycznych.
2. Instrukcja została opracowana zgodnie z wymogami § 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. Nr 100, poz. 1024).
3. Podstawowymi celami zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych, jest zapewnienie jak najwyższego poziomu bezpieczeństwa przetwarzanych danych osobowych w systemach informatycznych.
4. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania w systemach, charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności.
5. ABI powinien posiadać stosowne uprawnienia w nadzorowanych systemach informatycznych, gwarantujące skuteczne wykonywanie zadań z zakresu nadzoru wszędzie tam, gdzie jest to możliwe. Nie oznacza to automatycznego prawa dostępu do danych osobowych przetwarzanych w tych systemach.
6. Ilekroć w Instrukcji jest mowa o „**użytkowniku**” rozumie się przez to pracownika/współpracownika upoważnionego do przetwarzania danych osobowych w systemie informatycznym Urzędu.

§ 2

Szkolenia w zakresie ochrony danych osobowych

1. Użytkownicy powinni podlegać okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

§ 3

Obowiązki Administratora Bezpieczeństwa Informacji

Do obowiązków ABI w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

- 1) nadzór nad stosowaniem zabezpieczeń danych w systemach informatycznych;
- 2) wskazywanie zagrożeń oraz reagowanie na naruszenia ochrony danych osobowych i usuwanie ich skutków;
- 3) prowadzenie ewidencji użytkowników systemów informatycznych, w których przetwarzane są dane osobowe, stanowiącej część ewidencji osób upoważnionych do przetwarzania danych osobowych w Urzędzie;
- 4) kontrolowanie nadanych w systemach informatycznych uprawnień do przetwarzania danych osobowych pod kątem ich zgodności z wpisami umieszczonymi w ewidencji osób upoważnionych do przetwarzania danych osobowych;

- 5) prowadzenie szkoleń dla użytkowników w zakresie stosowanych zabezpieczeń danych w systemach informatycznych;
- 6) uzgadnianie z ASI szczególnych procedur regulujących wykonywanie czynności w systemach służących do przetwarzania danych osobowych w Urzędzie;
- 7) zapewnienie doradztwa w zakresie przestrzegania przez współpracowników zasad ochrony danych osobowych przyjętych w Urzędzie Miasta Pionki.

§ 4

Obowiązki Administratora Systemów Informatycznych

Do obowiązków Administratora Systemów Informatycznych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

- 1) realizacja zadań określonych w § 6, § 9, § 23 i § 24 Polityki;
- 2) operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych;
- 3) przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa;
- 4) kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym Administratora Danych;
- 5) zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień na podstawie zaakceptowanych wniosków przez osobę do tego upoważnioną;
- 6) utrzymanie systemu w należytej sprawności technicznej;
- 7) regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych;
- 8) wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe.

§ 5

Obowiązki właścicieli zasobów danych osobowych

Do obowiązków właścicieli zasobów danych osobowych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

- 1) zapewnienie, we współpracy z ASI, właściwego poziomu ochrony danych osobowych w systemach, dla danych za które są odpowiedzialni;
- 2) informowanie ABI o zmianie celu przetwarzania danych osobowych w systemie lub poszerzeniu zakresu zbieranych danych osobowych, udostępnianie danych osobowych wyłącznie osobom upoważnionym lub uprawnionym do ich uzyskania.

§ 6

Obowiązki użytkowników

Do obowiązków użytkowników w zakresie ochrony danych osobowych w systemach informatycznych należy w szczególności:

- 1) przestrzeganie opracowanych dla systemu zasad przetwarzania danych osobowych;
- 2) przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa;
- 3) uniemożliwienie dostępu lub podglądu danych osobowych w systemie dla osób nieupoważnionych;

- 4) wykonywania bez zbędnej zwłoki poleceń ABI i ASI w zakresie ochrony danych osobowych, jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

§ 7

Bezpieczna eksploatacja systemów informatycznych

1. Jeżeli nic innego nie wynika z przepisów niniejszej Instrukcji użytkownikom zabrania się:
 - 1) wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie;
 - 2) umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych;
 - 3) instalowania nowego lub aktualizowania już zainstalowanego oprogramowania;
 - 4) korzystania z systemów informatycznych dla celów innych niż związane z wykonywaniem obowiązków służbowych;
 - 5) korzystania z prywatnego sprzętu informatycznego, w tym oprogramowania oraz nośników pamięci;
 - 6) podejmowania prób testowania, modyfikacji i naruszenia zabezpieczeń danych w systemach informatycznych lub jakichkolwiek działań noszących takie znamiona;
 - 7) kopiowania plików zawierających dane osobowe z serwerów na stacje robocze użytkowników i na elektroniczne nośniki informacji, chyba że zgodę na te działania wyrazi ABI.
2. Informacje przetwarzane przy użyciu współdzielonych aplikacji sieciowych na stacjach roboczych muszą być zapisywane na dyskach serwera.
3. Wszystkie aplikacje sieciowe, współdzielone zasoby użytkowe muszą być ulokowane na przeznaczonych do tego celu serwerach.

§ 8

Nadawanie uprawnień do przetwarzania danych osobowych

1. Użytkownicy przed przystąpieniem do przetwarzania danych osobowych w systemie informatycznym, zobowiązani są zapoznać się z:
 - 1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2016 r. poz. 922 z późn. zm.);
 - 2) Polityką bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta Pionki;
 - 3) niniejszą Instrukcją.
2. Użytkownicy przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe powinni podlegać przeszkoleniu w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będą wykorzystywali.
3. Odpowiedzialnym za zgłoszenie użytkownika do szkolenia, o którym mowa w ust. 2, jest jego kierownik.
4. Pierwsze zarejestrowanie użytkownika w systemie i nadanie odpowiednich uprawnień do systemu przetwarzającego dane osobowe musi być poprzedzone złożeniem przez niego oświadczenia o:
 - 1) zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczania oraz przetwarzaniu danych osobowych zgodnie z przepisami;
 - 2) uzyskanie formalnego upoważnienia do przetwarzania danych osobowych;
5. Po spełnieniu wymagań określonych w ust. 4, rejestrowanie użytkowników i nadawanie im uprawnień w systemach informatycznych należy realizować zgodnie z procedurą określoną w § 15 Polityki.

6. Zakres dostępu użytkownika powinien być rejestrowany w ewidencji osób upoważnionych do przetwarzania danych osobowych, określonej w § 16 Polityki.
7. ASI powinien przekazywać użytkownikowi tymczasowe hasło dostępowe w sposób zapewniający ich poufność (np. w zaklejonej taśmą kopercie).
8. Procedurę nadawania uprawnień do przetwarzania danych osobowych w systemach należy stosować odpowiednio, w przypadku zmiany uprawnień w systemach lub w przypadku odebrania uprawnień w systemach.
9. Zmiany dotyczące użytkowników, takie jak rozwiązanie umowy o pracę, umowy o współpracę lub utrata upoważnienia, są przesłanką do natychmiastowego wyrejestrowania ich z systemu informatycznego służącego do przetwarzania danych oraz unieważnienia hasła i odnotowanie tego faktu w ewidencji osób upoważnionych do przetwarzania danych osobowych, o której mowa w ust. 6.
10. Właściciel zasobu danych osobowych jest zobowiązany niezwłocznie po zaistnieniu okoliczności, o których mowa w ust. 9, zgłosić je na piśmie do ABI.
11. W przypadku długotrwałej absencji użytkownika, w celu zablokowania możliwości logowania się do jego konta, stosuje się odpowiednio przepisy ust. 10.
12. Przy podejmowaniu decyzji co do okresu przyznawania uprawnień w systemie informatycznych należy się kierować charakterem zatrudnienia użytkownika w Urzędzie oraz przewidywanemu okresowi, na jaki dostęp do systemu będzie mu niezbędny w celu wykonania powierzonych zadań.
13. Dostęp do systemu informatycznego, a także do poszczególnych aplikacji i baz danych przetwarzających dane osobowe powinien być możliwy tylko po podaniu identyfikatora odrębnego dla każdego pracownika/współpracownika i poufnego hasła.

§ 9

Metody i środki uwierzytelniania w systemie

1. Identyfikatory i hasła są środkiem gwarantującym rozliczalność, poufność i integralność danych osobowych przetwarzanych w systemach informatycznych. Służą one do weryfikowania tożsamości pracownika/współpracownika, uzyskania dostępu do określonych zasobów, kont uprzywilejowanych lub uruchomienia określonej funkcjonalności.
2. Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania pełnej rozliczalności wykonywania operacji w systemach informatycznych, wszyscy użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:
 - 1) użytkownik systemu powinien posiadać unikalny identyfikator do swojego osobistego i wyłącznego użytku;
 - 2) hasła dostępu do systemów informatycznych powinny być tworzone przez użytkownika i stanowią tajemnicę służbową, znaną wyłącznie temu użytkownikowi z zastrzeżeniem § 8 ust. 7;
 - 3) użytkownik ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie;
 - 4) hasła nie mogą być ujawniane lub przekazywane komukolwiek, bez względu na okoliczności;
 - 5) użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach, programach które umożliwiają zapis loginów i haseł lub pod klawiszami funkcyjnymi).
3. Użytkownicy są co do zasady odpowiedzialni za wszelkie działania w systemach informatycznych prowadzone z użyciem ich identyfikatora i hasła.

4. ASI jest odpowiedzialny za okresowe sprawdzanie systemu pod kątem występowania w nim nieaktywnych kont użytkowników.

§ 10

Wymogi dotyczące uwierzytelniania

1. Wszystkie konta dostępowe (identyfikatory) do systemów informatycznych powinny być chronione hasłem lub innym bezpiecznym, zaakceptowanym przez ABI sposobem uwierzytelniania.
2. Identyfikator oraz nadane uprawnienia powinny umożliwiać wykonywanie czynności wyłącznie zgodnych z zakresem powierzonych obowiązków.
3. Identyfikator użytkownika powinien być niepowtarzalny a po wyrejestrowaniu z systemu informatycznego lub utracie ważności nie może być przydzielany innej osobie.
4. Hasło początkowe, które jest przydzielane przez ASI, powinno umożliwiać użytkownikowi zarejestrowanie się w systemie tylko jeden raz i powinno być natychmiast zmienione przez użytkownika.
5. Użytkownicy powinni wybierać hasła dobrej jakości składające się co najmniej z 8 znaków, zawierające kombinację małych i wielkich liter oraz cyfry.
6. Hasła nie mogą być takie same jak identyfikator użytkownika oraz nie mogą być zapisywane w systemach w postaci jawnej.
7. Hasła powinny być utrzymywane w tajemnicy również po upływie ich ważności.
8. Należy unikać ponownego używania starych haseł.
9. Użytkownicy o wysokich uprawnieniach (np. root, administrator) nie powinni wykorzystywać swojego konta do przetwarzania danych osobowych w systemie. Jeśli zajdzie potrzeba przetwarzania danych przez użytkownika o wysokich uprawnieniach, powinno zostać założone dla niego odrębne konto, które nie będzie związane z wysokimi uprawnieniami.
10. Hasła użytkowników o wysokich uprawnieniach powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób nieupoważnionych.
11. Udostępnienie hasła osobie postronnej należy traktować jako incydent naruszenia ochrony danych osobowych.

§ 11

Wymogi dotyczące zmiany haseł

1. Użytkownik jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje:
 - 1) okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła), nie rzadziej niż co 30 dni;
 - 2) 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 pisemnie o zmianę hasła do Administratora Systemów Informatycznych, w sytuacji:
 - 1) zapomnienia/zgubienia hasła;
 - 2) wygaśnięcia ważności hasła;
 - 3) zablokowania konta spowodowanego nieprawidłowym wprowadzeniem hasła;
 - 4) braku uprawnień/interfejsu umożliwiających samodzielną zmianę hasła.

§ 12

Procedura bezpiecznego uwierzytelniania

1. Procedura bezpiecznego uwierzytelniania w systemie informatycznym zapewnia minimalizowanie ryzyka wystąpienia nieautoryzowanego dostępu do systemu. Procedura powinna ujawniać minimum informacji o systemie informatycznym tak, aby nie pozwolić nieuprawnionemu użytkownikowi na uzyskanie dodatkowych wskazówek w celu ich wykorzystania w sposób niedozwolony. W tym celu należy zapewnić:
 - 1) zatwierdzanie jedynie kompletnych informacji wejściowych, niezbędnych przy logowaniu jeżeli wystąpi błąd, system nie powinien wskazywać, która część danych jest poprawna, a która niepoprawna;
 - 2) ograniczenie liczby nieudanych prób logowania się do systemu do najwyżej trzech prób, oraz uwzględnić:
 - a) wykonywanie zapisu nieudanych i udanych prób,
 - b) wymuszanie odstępu czasowego przed każdą kolejną próbą logowania się lub odrzucanie wszelkich dalszych prób, jeśli nie mają specjalnej autoryzacji,
 - c) rozłączenie połączeń,
 - d) ustawienia maksymalnej liczby prób logowania się w połączeniu z minimalną długością hasła oraz wartością chronionego systemu,
 - e) ograniczenie maksymalnego i minimalnego czasu trwania logowania; jeśli zostanie on przekroczony, system powinien przerwać procedurę logowania,
 - 3) wyświetlanie się po pomyślnym zalogowaniu daty i czasu ostatniego pomyślnego logowania do systemu;
 - 4) blokowanie wyświetlania hasła w trakcie wprowadzania lub ukrywanie wprowadzanych znaków pod symbolami;
 - 5) blokowanie przesyłania niezaszyfrowanych haseł przez sieć.

§ 13

Wymagania dotyczące sprzętu i oprogramowania

1. Wygaszacz stacji roboczej powinien być skonfigurowany w taki sposób, aby aktywował się automatycznie po upływie 15 minut od ostatniego użycia stacji roboczej, uruchamiając blokadę
2. Dane osobowe wyświetlane na ekranach monitorów należy zabezpieczyć w taki sposób, by uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora.
3. Programy zainstalowane na stacjach roboczych stacjonarnych i na komputerach przenośnych obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.
4. Oprogramowanie może być używane tylko zgodnie z prawami licencji. Oprogramowanie typu Freeware, Shareware lub inne oprogramowanie dostarczane bez opłat jest uznawane jako nieautoryzowane, jeżeli nie otrzyma stosownej aprobaty Administratora Danych.
5. Przed zainstalowaniem nowego oprogramowania ASI lub inna upoważniona osoba, zobowiązana jest sprawdzić jego działanie pod kątem bezpieczeństwa całego systemu.
6. Sieć teleinformatyczna wykorzystywana do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu informatycznego.
7. Serwer systemu przetwarzającego dane osobowe i urządzenia NAS powinny być zasilane przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie zasilania przez co najmniej 15 minut oraz na wykonanie, bezpiecznego wyłączenia serwera, tak aby przed

- ostatecznym zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na zbiorze danych osobowych.
8. Pomieszczenie serwerowni oraz pomieszczenia, w których przetwarzane są dane osobowe powinny być odpowiednio chronione przed skutkami pożaru.
 9. Infrastruktura techniczna związana z siecią teleinformatyczną i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.
 10. Gniazda zasilania sieci teleinformatycznej powinny być odpowiednio oznakowane, zabezpieczone przed włączeniem do nich innych odbiorników i wykonane w specjalnym standardzie.
 11. Należy chronić informacje zawarte w dziennikach zdarzeń systemów przed manipulacją i nieautoryzowanym dostępem.
 12. Należy zapewnić synchronizację zegarów wszystkich stosowanych systemów służących do przetwarzania danych osobowych z uzgodnionym, dokładnym źródłem czasu.
 13. Należy zapewnić aby porty i usługi, które nie są wykorzystywane były zablokowane.

§ 14

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. 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.
3. 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.
4. 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.
5. Treść ostatecznego rozstrzygnięcia indywidualnej sprawy osoby, której dane dotyczą, nie może być wyłącznie wynikiem operacji na danych osobowych, prowadzonych w aplikacji lub systemie informatycznym.
6. Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w aplikacjach ewidencjonujących osoby fizyczne
7. Zaleca się wbudowanie do aplikacji funkcjonalności, zapewniających wymuszanie zmiany haseł po zadany czasie, badania ich długości, jakości i powtarzalności (z użyciem funkcji skrótu).

§ 15

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 postępować zgodnie z procedurą opisaną w § 21 Polityki.
3. Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest zablokować swoją stację roboczą.
4. 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.

§ 16

Przetwarzanie, udostępnianie i likwidacja 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.W zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.
2. Kopiowanie przez użytkowników plików z serwerów na stacje robocze użytkowników i na elektroniczne nośniki informacji jest zabronione bez akceptacji ze strony ABI.
3. W przypadku udostępniania danych osobowych odbiorcy danych w rozumieniu art. 7 pkt 6 ustawy, użytkownik ma obowiązek odnotować komu i kiedy udostępniono poszczególne dane.
4. Jeżeli dane osobowe nie są pozyskane od osoby, której dotyczą, użytkownik zobowiązany jest odnotować w systemie informatycznym źródło pochodzenia danych.
5. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych nie podlegających archiwizacji w odrębnym trybie dla którego cel przetwarzania ustał, ABI 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.
6. Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w systemach informatycznych podejmują właściciele zasobów.
7. 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.

8. Przed przekazaniem elektronicznego nośnika informacji osobie nieuprawnionej, należy usunąć z nośnika w sposób trwały dane osobowe.

§ 17

Kopie zapasowe

1. Kopie zapasowe zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania powinny być wykonywane - zgodnie z planem wykonywania kopii zapasowych - przez ASI.
2. ASI zapewnia utworzenie dokładnego i kompletnego spisu kopii zapasowych oraz procedur ich odtwarzania.
3. W celu usystematyzowania procesu wykonywania kopii zapasowej, odpowiedzialny za ten proces ASI, jest zobowiązany do sporządzenia harmonogramu wykonywania kopii 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.
4. Tworzenie, przechowywanie i likwidację kopii zapasowych powinny regulować szczegółowe instrukcje operacyjne dla poszczególnych systemów informatycznych, opracowywane przez ASI, z uwzględnieniem niniejszych postanowień.
5. ASI odpowiedzialny za tworzenie kopii 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.
6. Kopie zapasowe powinny być tworzone w bezpiecznym systemie archiwizacji, który powinien zapewniać ograniczony dostęp fizyczny do nośników oraz przyznanie uprawnień dostępu tylko wyznaczonemu imiennie ASI oraz ABI.
7. Dane z kopii zapasowych powinny być odtwarzane wyłącznie przez ASI oraz upoważnionych przez Administratora Danych pracowników.
8. Kopie zapasowe, które uległy uszkodzeniu powinny podlegać natychmiastowemu zniszczeniu.
9. Zakwalifikowanie uszkodzonych nośników elektronicznych do zniszczenia dokonuje ASI lub inna upoważniona przez Administratora Danych osoba.
10. Proces niszczenia kopii zapasowych powinien odbywać się komisyjnie i powinien być dokumentowany.

§ 18

Przechowywanie nośników elektronicznych zawierających dane osobowe

1. Dane osobowe mogą być przechowywane:
 - 1) na serwerach zlokalizowanych w obszarach wyznaczonych do przetwarzania danych osobowych;
 - 2) na wymiennych nośnikach elektronicznych;
 - 3) na poszczególnych stacjach roboczych.
2. Po wykorzystaniu dane osobowe w postaci elektronicznej należy niezwłocznie usunąć z nośnika elektronicznego w sposób uniemożliwiający ich ponowne odtworzenie.
3. Wykorzystanie wymiennych nośników elektronicznych (CD/DVD, pamięć USB, wymienna karta pamięci, dyskietka) powinno być ściśle kontrolowane i dozwolone wyłącznie dla upoważnionych użytkowników.
4. Wymienne nośniki elektroniczne, o ile nie są użytkowane, powinny być przechowywane w zamykanych szafkach.

5. Nośniki zawierające kopie zapasowe powinny być przechowywane w innym pomieszczeniu niż to, w którym umieszczony jest serwer przetwarzający dane osobowe.
6. Kopie zapasowe powinny być przechowywane w odpowiednio zabezpieczonej, ognioodpornej szafie, do której dostęp mogą mieć wyłącznie osoby upoważnione.
7. Nośniki elektroniczne z danymi osobowymi powinny być:
 - 1) oznaczane i przechowywane w zamykanych szafach lub sejfach;
 - 2) przechowywane maksymalnie przez okres wskazany dla danego rodzaju danych osobowych przez Administratora Bezpieczeństwa Informacji.
8. Informację o maksymalnym okresie przechowywania nośników magnetycznych oraz optycznych, na których zapisane są dane osobowe przekazują Właściciele zasobów danych osobowych do Administratora Bezpieczeństwa Informacji.

§ 19

Ochrona systemu informatycznego przed działaniem szkodliwego oprogramowania

1. Na każdej stacji roboczej w sieci oraz serwerze przetwarzającym dane osobowe powinno być zainstalowane oprogramowanie antywirusowe skanujące na bieżąco system informatyczny.
2. Skaner poczty elektronicznej powinien być stale włączony.
3. Oprogramowanie antywirusowe powinno być zainstalowane tak, aby użytkownik nie był w stanie wyłączyć lub pominąć etapu skanowania.
4. Kontrola antywirusowa powinna być przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
5. Należy stosować wersje programów antywirusowych z aktualną bazą sygnatur wirusów.
6. Nowe wersje oprogramowania antywirusowego oraz uaktualnienia bazy sygnatur wirusów instalują ASI niezwłocznie po ich otrzymaniu lub ściągnięciu, uprzednio weryfikując pochodzenie oprogramowania.
7. W razie zainfekowania systemu ASI odpowiada za usunięcie wirusa.
8. ASI ma prawo odłączyć od sieci stację roboczą, na której zostanie zlokalizowany wirus, jeśli uzna, że dalsze pozostawienie jej w sieci zagraża innym stacjom roboczym.

§ 20

Zasady komunikacji w sieci teleinformatycznej

1. Przesyłanie danych osobowych drogą teletransmisji powinno odbywać się wyłącznie przy wykorzystaniu wymaganych zabezpieczeń logicznych chroniących przed nieuprawnionym dostępem, w szczególności takich jak ochrona kryptograficzna.
2. Wyłącznie w sytuacjach wyjątkowych dopuszcza się przetwarzanie danych osobowych w plikach (MS Word, MS Excel) na stacjach roboczych użytkowników, poza bazą danych, znajdującą się w określonym systemie informatycznym. Powyższe zastrzeżenie nie obowiązuje w przypadku przetwarzania danych osobowych przy użyciu programów komputerowych wyłącznie do edycji tekstu, w celu udostępnienia danych osobowych na piśmie.
3. Zgodę na przetwarzanie danych w sytuacjach określonych w ust. 2 wydają właściciele zasobów danych osobowych.
4. Inne technologie sieciowe takie jak sieci lokalne oparte na falach radiowych nie mogą być wykorzystywane do przekazu informacji, o ile połączenie nie jest szyfrowane. Takie połączenia mogą być używane jedynie dla wymiany poczty elektronicznej o ile wiadomo, że nie zawiera ona danych osobowych.

5. Wszystkie połączenia zewnętrzne do systemu informatycznego powinny być monitorowane, a logi połączeń archiwizowane w trybie ciągłym i usuwane po 12 miesiącach.
6. System informatyczny służący do przetwarzania danych osobowych, powinien być chroniony przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
7. Zabezpieczenia logiczne, o których mowa w ust. 7 powyżej, obejmują:
 - 1) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną;
 - 2) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
8. Zdalne uruchamianie komend systemowych ze stacji roboczych znajdujących się w lokalizacjach nienależących do Urzędu jest możliwe, po prawidłowym logowaniu się użytkownika i zastosowaniu „silnego” uwierzytelnienia, na przykład tokenów kryptograficznych, haseł jednorazowych, certyfikatów cyfrowych. (wystarczy po logowaniu)

§ 21

Zasady monitorowania, przeglądu i konserwacji systemu informatycznego

1. Przeglądy, naprawy i konserwacje systemu informatycznego, które będą przeprowadzane w miejscu użytkowania tego systemu wymagają obecności ASI lub innej wyznaczonej osoby.
2. Za prawidłowość przeprowadzenia przeglądów, zapewnienia jakości, konserwację i dokumentowanie zmian w systemach odpowiada ASI.
3. W przypadku gdy konieczne jest dokonanie przeglądu, naprawy lub konserwacji systemu informatycznego poza miejscem jego użytkowania, z urządzenia należy wymontować element, na którym zapisane są dane osobowe, o ile jest to możliwe. W przeciwnym wypadku należy zawrzeć z podmiotem dokonujący naprawy umowę powierzenia w rozumieniu art. 31 ustawy o ochronie danych osobowych.
4. Przegląd programów i narzędzi programowych powinien być przeprowadzany w przypadku zmiany wersji oprogramowania aplikacji, zmiany wersji oprogramowania bazy danych lub wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.
5. Codziennie ASI powinien przeprowadzać kontrolę logów zdarzeń zachodzących w systemie.
6. Raz do roku należy przeprowadzać weryfikację całego oprogramowania użytkowego eksploatowanego na wszystkich stacjach roboczych podłączonych do systemu informatycznego pod kątem spełnienia wymogów bezpieczeństwa.

§ 22

Zasady postępowania z komputerami przenośnymi

1. Osoba używająca komputer przenośny zawierający dane osobowe zobowiązana jest zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych.
2. Osoba używająca komputer przenośny zawierający dane osobowe w szczególności powinna:
 - 1) stosować ochronę kryptograficzną wobec danych osobowych przetwarzanych na komputerze przenośnym;
 - 2) zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego - identyfikator i hasło;
 - 3) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych;
 - 4) nie wykorzystywać komputera przenośnego do przetwarzania danych osobowych w obszarach użyteczności publicznej;

- 5) zachować szczególną ostrożność przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych.
3. W przypadku podłączania komputera przenośnego do sieci publicznej poza siecią Urzędu należy zastosować firewall zainstalowany bezpośrednio na tym komputerze oraz system antywirusowy.
4. Użytkownik powinien zachować wyjątkową ostrożność podczas korzystania z zasobów sieci publicznej.
5. Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego formalny użytkownik.

§ 23

Postanowienia końcowe

1. ABI zobowiązany jest zapoznać z treścią Instrukcji każdego użytkownika systemu informatycznego służącego do przetwarzania danych osobowych.
2. W sprawach nieuregulowanych w Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (tj. Dz. U. z 2016 r., poz. 922 z późn. zm.) oraz przepisy wykonawcze do tejże Ustawy.

Zatwierdził:

BURMISTRZ

Romuald Zawodnik

