ZARZĄDZENIE Nr 7.2015
Burmistrza Miasta Zawidowa
z dnia 12-02-2015

w sprawie: wprowadzenia Polityki Bezpieczeństwa danych osobowych i systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Zawidowie.

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 poz. 1182 i 1662) i § 3, § 4, § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 Nr 100, poz. 1024)

§ 1. Wprowadza się do użytku służbowego „Politykę Bezpieczeństwa danych osobowych i systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Zawidowie" w zakresie przetwarzania danych osobowych w Urzędzie Miejskim w Zawidowie stanowiącą załącznik nr 1 do niniejszego zarządzenia .

§ 2. Zobowiązuje się wszystkich pracowników Urzędu Miejskiego w Zawidowie oraz strony świadczące usługi na rzecz Urzędu Miejskiego w Zawidowie do przestrzegania przepisów zawartych w dokumentach, o których mowa w § 1.

§ 3. Wykonanie powierza się Sekretarzowi Miasta Zawidowa.

§ 4. Zarządzenie wchodzi z dniem wydania.

Burmistrz Miasta

Robert Gałuszny

POLITYKA BEZPIECZEő STAWA DANYCH OSOBOWYCH I SYSTEMÓW INFORMATYCZNYCH SĞUt ł CYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W URZŇDZIE MIEJSKIM W ZAWIDOWIE

Spis treści

Lista zaŁączników

ZaŁącznik nr 1: Wzór upowaŻnienia,

ZaŁącznik nr 2: Wzór oŚwiadczenia,

ZaŁącznik nr 3: Wzór wycofania upowaŻnienia,

ZaŁącznik nr 4: Ewidencja osób upowaŻnionych do przetwarzania danych,

ZaŁącznik nr 5: Wykaz budynków, pomieszczeŃ lub czĘŚci pomieszczeŃ, w których przetwarzane sŁdane,

ZaŁącznik nr 6: Wykaz zbiorów danych osobowych przetwarzanych w UrzĘdzie Miejskim,

ZaŁącznik nr 7: Sposób przepŁywu danych pomiĘdzy systemami,

ZaŁącznik nr 8: Opis struktury zbiorów danych,

ZaŁącznik nr 9: Wzór wykazu osób, które zapoznaŁy siĘ z dokumentem.

ZaŁącznik nr 10: Raport z naruszenia bezpieczeŃstwa systemu informatycznego

Postanowienia ogólne

Polityka bezpieczeństwa danych osobowych w Urzędzie Miejskim w Zawidowie zwana dalej „Polityką" została wydana 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.
Polityka została opracowana zgodnie z wymogami określonymi w § 4 i § 5 ww. rozporządzenia.

Podstawą prawną dla polityki bezpieczeństwa danych osobowych w Urzędzie Miejskim w Zawidowie stanowią:
1) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 r. poz. 1182 i 1162).
2) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr. 100, poz. 1024).

Definicje

Przez użyte w Polityce określenia należy rozumieć:

1. **Polityka** – rozumie się przez to Politykę Bezpieczeństwa danych osobowych w Urzędzie Miejskim w Zawidowie
2. **Administrator Danych Osobowych (ADO)** – rozumie się przez to jednostkę organizacyjna w imieniu, której działa Burmistrz Miasta.
3. **Administrator Bezpieczeństwa Informacji (ABI)** – pracownik UMZ, wyznaczony przez Burmistrza odpowiedzialny za organizację ochrony danych osobowych.
4. **Administrator Systemu Informatycznego (ASI)** – pracownik nadzorujący pracę systemu informatycznego w UMZ.
5. **Ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
6. **Rozporządzenie** – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jaki powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).
7. **Baza danych osobowych** – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest zbudowana z elementów o określonej strukturze – rekordów lub obiektów.
8. **Dane osobowe (dane)** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby.
9. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znanych jedynie osobie uprawnionej do pracy w systemie informatycznym.
10. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
11. **Integralność danych** – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
12. **Nośnik komputerowy** – nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyski twarde.
13. **Odbiorca danych** – każdy, komu udostępnia się dane osobowe z wyjątkiem:
    - osoby, której dane dotyczą,
    - osoby upoważnionej do przetwarzania danych;

- podmiotu, o którym mowa w art. 31 ustawy;
- przedstawiciela, o którym mowa w art. 31a ustawy;
- organów państwowych lub organu samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

14. **Poufność danych** – właściwość zapewniająca, że dane są udostępniane nieupoważnionym podmiotom.
15. **Przetwarzanie danych** – wykonywania jakiejkolwiek operacji na danych osobowych np. zbieranie, utrwalanie, opracowywanie, udostępnianie zmienianie, usuwanie.
16. **Raport** – przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzania danych.
17. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
18. **Usuwanie danych**- zniszczenie danych osobowych lub takich ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą
19. **Uwierzytelnienie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
20. **Użytkownik** – pracownik UMZ posiadający uprawnienia do przetwarzania danych osobowych w zakresie obowiązujących przepisów o ochronie danych osobowych.
21. **Zabezpieczenia danych w systemie informatycznym** – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
22. **Zbiór danych** – zestaw danych osobowych posiadających określoną strukturę, prowadzony według określonych kryteriów oraz celów np. zbiór pracowników UMZ, zbiór interesantów UMZ.
23. **Zgoda osoby, której dane dotyczą** – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana z oświadczenia woli o innej treści.

Rozdział I

Cele i zakres polityki bezpieczeństwa

1. Polityka wprowadza się w celu zapewnienia ochrony danych osobowych przetwarzanych przez Urząd Miejski w Zawidowie przed wszelkiego rodzaju zagrożeniami zewnętrznymi jak i wewnętrznymi.

   PB ma zastosowanie w stosunku do wszystkich danych osobowych niezależnie od formy jej przetwarzania, udostępniania i przechowywania.
2. Zakres przedmiotowy niniejszej polityki obejmuje dane osobowe przetwarzane w Urzędzie niezależnie od formy ich przetwarzania, udostępniania i przechowywania, zarówno w formie elektronicznej, jak i tradycyjnej.
3. Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczenia, jako zestaw praw, reguł i zaleceń, regulujących sposób ich zarządzania, ochrony i dystrybucji wewnątrz Urzędu. Zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych.
4. Ochrona danych jest realizowana poprzez zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
5. Polityka obowiązuje wszystkich pracowników Urzędu oraz podmiotów współpracujących na zasadzie umów, mających jakikolwiek kontakt z danymi osobowymi objętymi ochroną
6. Bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pacy, zasady określone niniejszej polityce oraz w dokumentach powiązanych powinny być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez współpracowników przetwarzających dane osobowe, których administratorem jest Gmina Miejska Zawidów w imieniu której działa Burmistrz Miasta Zawidowa.

Rozdział II

Zadania i uprawnienia ADO, ABI i ASI.

1. Administrator Danych Osobowych, którym jest Burmistrz, zarządzeniem wyznacza Administratora Bezpieczeństwa Informacji w celu organizacji ochrony danych osobowych oraz Administratora Systemu Informatycznego dla danych zawartych w systemach informatycznych Urzędu Miejskiego.
2. Administrator Danych Osobowych jest odpowiedzialny za przetwarzanie i ochronę danych osobowych zgodnie z przepisami prawa oraz realizuje zadania w zakresie ochrony danych osobowych.
3. Do obowiązków ADO należy:
   - Wyznaczenie Administratora Bezpieczeństwa Informacji, Administratora Systemu Informatycznego.
   - zapewnienie odpowiednich pomieszczeń, stosownie zabezpieczonych i wyposażonych do przetwarzania i przechowywania danych osobowych, zaznajomienie pracowników z prawnymi oraz pracowniczymi konsekwencjami naruszenia bezpieczeństwa danych osobowych.
   - Podejmowanie decyzji o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych.
   - Podejmowanie odpowiednich działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.
   - Zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem.
   - Nadawanie upoważnień pracownikom Urzędu oraz użytkownikom zewnętrznym do przetwarzania danych.
   - Rejestracji w Głównym Inspektoracie Ochrony Danych Osobowych zbiorów danych przed przystąpieniem do ich przetwarzania, prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych.
   - Zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, w których przetwarzane są dane osobowe.
   - Zapewnienie środków finansowych niezbędnych do ochrony danych osobowych przetwarzanych w systemach informatycznych i zbiorach nieinformatycznych.

- Zapewnienie środków finansowych na merytoryczne przygotowanie osób odpowiedzialnych za nadzór nad ochroną danych.

4. Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad przetwarzania i ochrony danych osobowych w imieniu i na rzecz ADO
5. Do obowiązków ABI należy:
   - Sprawowanie nadzoru nad wdrożeniem stosowanych środków fizycznych, a także organizacyjnych, w celu zapewnienia bezpieczeństwa danych zgodnie z wymogami ustawy.
   - Zapewnienie przetwarzania danych zgodnie z uregulowaniami niniejszej polityki.
   - Nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych na wniosek Właścicieli zasobów po akceptacji ADO dla pracowników oraz użytkowników zewnętrznych.
   - Przygotowywanie zgłoszeń zbiorów danych osobowych do rejestracji.
   - Prowadzenie „Ewidencji osób upoważnionych do przetwarzania danych osobowych".
   - Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych.
   - Nadzór nad bezpieczeństwem danych osobowych.
   - Inicjowanie i podejmowanie przedsięwzięć z zakresu doskonalenia ochrony danych osobowych w Urzędzie.
6. Administrator Bezpieczeństwa Informacji ma prawo:
   - Wstępu do pomieszczeń, w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą
   - żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego.
   - żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli.
   - żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.
7. Administratora Systemu Informatycznego realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora Danych.
   Rolę ASI pełni pracownik wyznaczony przez Administratora Danych Osobowych.
8. Do obowiązków ASI należy:

- Bieżący nadzór oraz zapewnienie optymalnej ciągłości działania systemu informatycznego, w tym opracowanie procedur określających zarządzanie systemem informatycznym przetwarzającym dane.
- Bezzwłoczne reagowanie w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych.
- Przeciwdziałanie próbom naruszenie bezpieczeństwa danych osobowych.
- Analizę raportów wszelkich zdarzeń, w tym incydentów związanych z bezpieczeństwem systemów przetwarzania danych.
- Zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych z Ustawą oraz niniejszą Polityką
- Instalacje i konfiguracje oprogramowania sprzętu sieciowego i serwerowego używanego do przetwarzania danych osobowych.
- Konfiguracja i administracja oprogramowania systemowego i sieciowego zabezpieczającego dane osobowe przez nieupoważnionych dostępem.
- Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania.
- nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teleinformatycznych.
- Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe.
- świadczenie pomocy technicznej w ramach oprogramowania, a także serwis sprzętu komputerowego będącego na stanie Urzędu Miejskiego w Zawidowie, służącego do przetwarzania danych osobowych.
- Diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacje omów z firmami świadczącymi usługi pogwarancyjnego sprzętu komputerowego.
- Wykonanie i zarządzanie kopiami awaryjnymi oprogramowania systemowego i sieciowego, w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie.
- Nadzór nad wdrożeniem i zarządzaniem aplikacji, w których przetwarza się dane osobowe.

9. Kierownicy referatów Urzędu Miejskiego są zobowiązani do:
   - Współdziałania z ABI w zakresie przestrzegania instrukcji, o której mowa w **rozdziale VI,**

- Sprawowania nadzoru nad pracą podległych pracowników w zakresie wykonywania czynności służbowych w sposób zapewniający ochronę danych osobowych,
- Zwracania się do ADO o rozstrzygniecie w przypadku istotnych wątpliwości co do stosowania przepisów prawnych zakresu danych osobowych,
- Niezwłocznego zawiadomienia ADO o konieczności utworzenia nowego zbioru danych osobowych, wymagającego rejestracji.

10. Pracownik upoważniony przez ADO do przetwarzania danych osobowych jest zobowiązany do:
    - Odbycia wewnętrznego szkolenia dotyczącego przetwarzania i ochrony danych osobowych,
    - Zapoznania się z przepisami prawa w zakresie ochrony danych osobowych, stosowania określonych przez ADO procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
    - Zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których te dane dotyczą,
    - Podporządkowania się poleceniom ABI oraz właściwego kierownika, w zakresie danych osobowych.
11. Czynności przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez ADO. Wzór upoważnienia stanowi **załącznik nr 1** do niniejszego dokumentu.
12. Pracownik, któremu ADO udzielił upoważnienia, o którym mowa w ust. 9 jest zobowiązany do podpisania oświadczenia. Wzór oświadczenia stanowi **załącznik nr 2** do niniejszego dokumentu.
13. Bezpośredni nadzór nad przetwarzaniem danych osobowych w komórkach organizacyjnych Urzędu Miejskiego sprawują kierownicy jednostek.
14. ADO może cofnąć upoważnienie, o którym mowa w ust.9. Wzór cofnięcia upoważnienie stanowi **załącznik nr 3** do niniejszego dokumentu.
15. Wypowiedzenie umowy o pracę jest równoznaczne z cofnięciem upoważnienia do przetwarzania danych osobowych.
16. Obowiązek przestrzegania tajemnicy danych osobowych spoczywa na pracownikach, którzy mają do nich dostęp, również po ustaniu stosunku pracy.

Rozdział III

Zasady przetwarzania danych.

1. Przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, gdy:
   - osoba, której dane dotyczą wyrazi zgodę, chyba, że chodzi o usunięcie jej danych,
   - jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
   - jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą jest stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
   - jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
   - jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.
2. Zgoda osoby, której dane dotyczą jest oświadczeniem woli, którego treścią jest zgoda na przetwarzanie jego danych osobowych w określonym celu, w określonym zakresie, przez określonego administratora danych osobowych. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. W przypadku zgody na przetwarzanie danych osobowych wrażliwych zgoda musi być wyrażona na piśmie.
3. W przypadku zbierania danych osobowych od osoby, której dane dotyczą należy zapewnić informacje dla tej osoby o:
   a) Nazwie i siedzibie administratora danych osobowych,
   b) Celu zbierania danych, a w szczególności o znanych lub przewidywanych odbiorcach danych osobowych,
   c) Prawie dostępu do treści swoich danych oraz ich poprawiania,
   d) Dobrowolności lub obowiązku podania danych osobowych, a jeżeli taki obowiązek istnieje o jego podstawie prawnej,
   e) Osobie przetwarzającej dane osobowe.

Rozdział IV

Opis zdarzeń naruszających ochronę danych osobowych

1. Podział zagrożeń:
   1) Zagrożenia losowe zewnętrzne (np. kliński żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłości systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
   2) Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych
   3) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia, naruszenia poufności danych (zazwyczaj nie następuje naruszenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.
2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:
   1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.
   2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych.
   3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru.
   4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu

5) jakoŚć danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenie systemu lub innć nadzwyczajnć i niepożądanć modyfikację w systemie
6) nastąpiło naruszenie lub próba naruszenia integralnoŚci systemu lub bazy danych w tym systemie
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji)
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicć procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.,
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. ‘bocznej furtki’
12) podmieniono lub zniszczono noŚniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe.
13) raża co naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenie z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.)

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowoŚci w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urzćdzenia archiwalne i inne) na noŚnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

Rozdział V
środki techniczne i organizacyjne stosowane w Urzędzie

1. Administrator danych osobowych jest zobowiązany do zachowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych w systemach informatycznych Urzędu, a w szczególności:
    1) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
    2) zapobiegać zabraniem danych przez osobę nieuprawnioną,
    3) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.
2. środki organizacyjne:
    1) dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia podpisane przez ADO,
    2) każdy z pracowników powinien zachować szczególną ostrożność przy przetwarzaniu, przenoszeniu wszelkich danych osobowych,
    3) należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych,
    4) pomieszczenia, w których przetwarzane są dane osobowe muszą być zamknięte na klucz,
    5) Dostęp do kluczy powinni posiadać tylko upoważnieni pracownicy,
    6) Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy Urzędu. W wypadku, gdy jest wymagany poza godzinami pracy - możliwy jest tylko na podstawie zezwolenia ADO,
    7) Dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy urzędu.
    8) W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonywanie niezbędnych czynności.
    9) Szafy, w których przechowywane są dane osobowe muszą być zamykane na klucz.
    10) Klucze do tych szaf powinni posiadać tylko upoważnieni pracownicy.
    11) Szafy z danymi powinny być otwarte tylko na czas potrzeby na dostęp do danych, a następnie powinny być zamykane.

12) Dane osobowe w formie papierowej mogĄznajdowaĆ siň na biurkach tylko na czas niezbňdny na dokonanie czynnoŜci sęuŻbowych, a nastňpnie muszĄbyĆ chowane do szaf.

3. ś rodki techniczne:
   1) dostňp do komputerów na których przetwarzane sĄdane osobowe mogĄmieĆ tylko upowaŻnieni pracownicy urzňdu.
   2) Stacje komputerowe, na których przetwarzane sĄdane osobowe powinny mieĆ ustawione tak monitory, aby osoby nieupowaŻnione nie miaęy wglĄdu w dane.
   3) KaŻdy plik, w którym zawarte sĄdane osobowe powinien byĆ zabezpieczony hasęem, jeŜli nie jest to przetwarzanie danych w systemie informatycznym.
   4) W przypadku przetwarzania danych osobowych na komputerach przenoŜnych naleŻy zachowaĆ szczególnĄostroŻnoŜĆ przy ich przenoszeniu.
   5) Po zakoŒczeniu pracy komputery przenoŜnie powinny byĆ zabezpieczone w zamykanych na klucz szafach.
   6) Komputerów tych nie moŻna wynosiĆ poza budynek Urzňdu.
   7) W przypadku potrzeby wyniesienia komputera przenoŜnego naleŻy dane osobowe przenieŜĆ na komputer stacjonarny w miejscu pracy.
   8) Nie naleŻy udostňpniaĆ osobom nieupowaŻnionym tych komputerów.
   9) W przypadku potrzeby przeniesienia danych osobowych pomiňdzy komputerami naleŻy dokonaĆ tego z zachowaniem szczególnej ostroŻnoŜci i za zgodĄABI.
   10) NoŜniki uŻyte do tego naleŻy wyczyŜciĆ, aby nie zostaęy na nich dane osobowe.
   11) W przypadku niemoŻliwoŜci skasowania danych z noŜnika naleŻy taki noŜnik zniszczyĆ fizycznie, za pomocĄodpowiedniej niszczarki.
   12) Niezabezpieczonych danych osobowych nie naleŻy przesyęaĆ drogĄelektronicznĄ
   13) SieĆ komputerowa powinna byĆ zabezpieczona przed wszelkim dostňpem z zewnĄrz.
   14) Do zabezpieczenia sieci naleŻy stosowaĆ:

       -firewall,

       - adresowanie stacji roboczych tylko adresami prywatnymi, nieroutowalnymi,

       - systemy wykrywania węamaŒIDS,

- logowanie wszelkich zdarzeń w dziennikach systemowych na serwerach i stacjach roboczych,
- systemy antywirusowe i antyszpiegowskie,
- zabezpieczenia skrzynek poczty elektronicznej hasłami trudnymi (min. 8 znaków, w tym litery, cyfry, znaki dodatkowe),
-zabezpieczenia stacji roboczych poprzez hasła w BIOS, w systemach MS Windows XP, Windows 7 (autoryzacja użytkownika, login + hasło),
- zabezpieczenie wszelkich systemów teleinformatycznych hasłami trudnymi (min. 8 znaków, w tym litery, cyfry, znaki dodatkowe) zmieniamy pierwszego dnia roboczego każdego miesiąca,
- ustawienie odpowiednich poziomów dostępu dla odpowiednich użytkowników w systemach teleinformatycznych, zmiany mogą zostać przeprowadzone tylko i wyłącznie przez administratora danego systemu)

4. Wykaz pomieszczeń, w których przetwarzane są dane osobowe stanowi załącznik nr 5 do niniejszego dokumentu.
5. Wykaz zbiorów danych osobowych przetwarzanych elektronicznie lub w inny sposób stanowi załącznik nr 6 do niniejszego dokumentu.
6. Opis struktury zbiorów danych stanowi załącznik nr 7 do niniejszego dokumentu.
7. Sposób przepływu danych pomiędzy systemami stanowi załącznik nr 8 do niniejszego dokumentu.

Rozdział VI

Instrukcja określająca sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem bezpieczeństwa informacji

1. Określenie sposobu przydziału haseł dla użytkowników i częstotliwości ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności.
    - hasło nie powinno zawierać mniej niż 8 znaków,
    - hasło nie powinno być takie same jak identyfikator,
    - hasło musi być zmieniane przynajmniej raz w miesiącu przez użytkownika, ABI, lub automatycznie przez system,
    - użytkownikowi nie wolno zapisywać hasła na papierze,
    - użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności,
    - w przypadku czasowego opuszczenia stanowiska pracy, użytkownik powinien wylogować się z systemu, lub uruchomić wygaszasz ekranu zabezpieczony hasłem,
    - za gospodarkę hasłami odpowiedzialny jest ABI,
    - hasło przy wpisywaniu nie może być wyświetlane na ekranie,
    - dopuszcza się użycie czytników biometrycznych.
2. Określenie sposobu rejestrowania i wyrejestrowania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności:
    - ABI prowadzi ewidencję osób upoważnionych do przetwarzania danych, **załącznik Nr 4** do niniejszego dokumentu.
    - rejestracji użytkowników w systemie dokonuje ABI, lub osoba przez niego upoważniona,
    - zarejestrować można wyłącznie osoby, które administrator danych wpisał do ewidencji osób upoważnionych do przetwarzania danych,
    - wyłączenie z ewidencji osób upoważnionych do przetwarzania danych, obliguje ABI do odebrania dostępu do danych osobowych,
3. Procedury rozpoczęcia i zakończenia pracy.
    - ABI w porozumieniu z kierownikiem referatu, ustala czas pracy użytkownikom systemu, na pracę poza godzinami funkcjonowania urzędu

musi wyrazić zgodę na piśmie kierownik jednostki, w formie upoważnienia jednorazowego lub stałego,

- ABI lub osoba przez niego upoważniona, nadzoruje rozpoczęcie i zakończenie pracy systemu informatycznego,
- w pomieszczeniach, gdzie przyjmowani są klienci, monitory powinny być tak ustawione, aby uniemożliwić osobie niepowołanej wgląd w dane,
- dopuszcza się pozostawienie włączonego serwera w nocy, jeżeli pomieszczenie, w którym on pracuje wyposażone jest w sprawny system oraz alarm antywłamaniowy,
- kontrola wprowadzanych danych prowadzona jest na bieżąco na każdym stanowisku merytorycznym, a nadzór prowadzi kierownik danej jednostki organizacyjnej,
- przekazaniu danych osobowych innym podmiotom decyduje ADO.

4. Metoda i częstotliwość tworzenia kopii awaryjnych
    - za sporządzenie i bezpieczeństwo kopii odpowiedzialny jest ABI i ASI, lub osoba upoważniona,
    - kopii należy dokonywać poprzez przegrywanie całej bazy danych,
    - w każdej chwili powinny być dostępne jednocześnie trzy kopie: z ostatnich 3 dni roboczych, miesiąca i roku. Kopie dzienne należy zapisywać na twardym dysku, a pozostałe na CD/DVD, bądź innym nośniku niemodyfikowalnym,
    - kopie awaryjne może tworzyć jedynie ABI i ASI, bądź osoba upoważniona,
    - w czasie tworzenia kopii awaryjnej przez ASI, dostęp do bazy danych dla wszystkich użytkowników powinien być zablokowany,
    - dyski wymienne z kopiami bezpieczeństwa powinny być wyjęte z komputera w czasie bieżącej pracy,
5. Wprowadza się praktyczne zalecenia odnośnie wykonywania kopii bezpieczeństwa:
    - przeprowadzać składowanie informacji regularnie,
    - używać różnych typów nośników danych,
    - kopie umieszczać w różnych, oddalonych od siebie miejscach,
    - najlepiej do składowania wybrać tak nośnik, aby mógł w całości pomieścić kopie danych,
    - przed składowaniem danych sprawdzić je programem antywirusowym,
    - dokładnie opisywać składowane dane,

- trzymać nośniki z kopiami z daleka od źródeł pola magnetycznego i miejsc nasłonecznionych,
- sprawdzić, czy składowanie przebiega prawidłowo,
- upewnić się, że nośnik jest niezależny od urządzenia, tzn. że dane mogą być przywrócone nie tylko na komputerze z którego były pobrane,
- regularnie konserwować urządzenia do składowania.

6. Metody i częstotliwość sprawdzania obecności wirusów komputerowych oraz sposoby ich usuwania
    - za ochronę antywirusową odpowiedzialny jest ASI,
    - do ochrony antywirusowej należy stosować program antywirusowy, zainstalowany na komputerze, gdzie odbierana jest poczta elektroniczna i sprawdzane są wszystkie nośniki wymienne, przed ich uruchomieniem w sieci oraz na komputerach stacjonarnych,
    - sprawdzanie dostępnymi programami antywirusowymi odbywać się powinno przynajmniej raz w tygodniu,
    - zalecane jest wykorzystanie programów pracujących w tle,
    - przy kontroli szczególną uwagę należy zwrócić na dokumenty pakietów biurowych,
    - każdą przesyłkę otrzymaną za pomocą transmisji danych należy sprawdzić programem antywirusowym,
    - korzystnie z zewnętrznych nośników i źródeł informacji może mieć miejsce wyłącznie po uzyskaniu zgody ABI,
    - w przypadku wykrycia wirusa choćby na jednym komputerze, należy sprawdzić wszystkie stacje robocze w urzędzie
7. Sposób i czas przechowywania nośników informacji, w tym kopii zapasowych i wydruków.
    - nie należy magazynować zbędnych plików i wydruków, kopie bezpieczeństwa po upływie okresu przechowywania muszą być skasowane, lub fizycznie zniszczone w sposób uniemożliwiający odczytanie danych,
    - za zniszczenie zbędnych wydruków i innych dokumentów zawierających dane osobowe odpowiedzialny jest kierownik referatu, za skasowanie danych lub zniszczenie nośników odpowiedzialny jest ASI,

- zbędne dokumenty papierowe powinny być zniszczone w niszczarce dokumentów lub przekazane do utylizacji firmie upoważnionej
- kopie bezpieczeństwa na nośnikach wymiennych powinny być przechowywane w zamkniętej metalowej szafie,
- kopie na nośnikach wymiennych nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowanych na bieżąco,
- kopie awaryjne sprawdza się pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu i co najmniej jednorazowo po przegraniu danych,
- wydruki należy przechowywać w pomieszczeniach, uniemożliwiających dostęp do niech przez osoby niepowołane,
- kopie przechowuje się co najmniej:
  - dziennie przez siedem dni,
  - tygodniowe przez kolejny tydzień,
  - miesięczne przez kolejny miesiąc,
  - roczne przez cały kolejny rok od daty sporządzenia.
- osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera w celu zapobieżenia dostępowi do tych danych osobie niepowołanej, powinna zabezpieczyć dostęp do komputera hasłem i nie zezwalać na użytkowanie komputera innym osobom.

8. Sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych
   - przeglądu i konserwacji dokonuje ASI, lub osoba upoważniona, przynajmniej dwa razy w roku,
   - zasilacz UPS powinien zapewnić automatyczne zakończenie pracy i wyłączenie serwerów przy zaniku lub nadmiernym wahaniu napięcia i min. czas podtrzymania pracy wynosi 5 minut,
   - w przypadku przekazywania komputera z dyskiem lub innym nośnikiem danych osobowych do naprawy, należy nośnik zdemontować, zabezpieczyć dostęp hasłem, dokonać naprawy w obecności osoby upoważnionej przez ADO lub przekazać do naprawy firmie, z którą Urząd podpisuje odpowiednie dokumenty przekazania zbioru danych z zastrzeżeniem, co do przetwarzania i

wykorzystania tych danych w przypadku przekazania nośnika innemu podmiotowi należy dane nieodwracalnie skasować,

- o wszelkich nieprawidłowościach, awariach, próbie lub naruszeniu bezpieczeństwa danych osobowych, użytkownik powinien niezwłocznie powiadomić ABI,
- do wydzielonej sieci energetycznej zasilającej system komputerowy nie wolno podłączać żadnych innych urządzeń,
- zabronione jest dokonywanie napraw sprzętu komputerowego samodzielnie przez pracowników urzędu.

9. Sposób postępowania w zakresie komunikacji w sieci komputerowej
    - system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych, lub logicznych zabezpieczeń, chroniących przed nieuprawnionym dostępem (załącznik do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 poz. 1024),
    - ABI z ADO określi zasoby dostępne dla każdego użytkownika,
    - użytkownicy powinni być przydzielani do odpowiedniej grupy roboczej, automatycznie w procesie logowania,
    - dostęp do serwerowi ma tylko ASI i pracownicy upoważnieni,
    - dostęp do konsoli serwera winien być zabezpieczony hasłem (min. 12 znaków),
    - - w pomieszczeniu, gdzie ustawiony jest serwer może pracować tylko ASI, lub osoby upoważnione,
    - nie wolno instalować na żadnym z komputerów w sieci urzędowej własnego oprogramowania bez zgody ASI,
    - użytkownicy nie uprawnieni nie powinni mieć dostępu do zasobów systemowych serwera. Katalogów roboczych, danych i woluminów z poziomu systemu operacyjnego,
    - dostęp do archiwalnych plików pocztowych, mających statut poufnych należy zabezpieczyć hasłem,
    - w celu zwiększenia bezpieczeństwa transmisji danych osobowych należy stosować kryptografie,

- w czasie korzystania z Internetu za pośrednictwem linii komutowanej, stacja powinna być fizycznie odłączona od sieci lokalnej,
- komunikacja w sieci lokalnej musi umożliwiać identyfikację pracujących użytkowników.

Rozdziaģ VII

Postępowanie w przypadku naruszenia ochrony danych osobowych.

1. Niniejsze zasady okreŚlajĄtryb postępowania w przypadku gdy:
    - stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie,
    - stan urzĄdzenia, zawartoŚĆ zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakoŚĆ komunikacji w sieci telekomunikacyjnej, mogĄ wskazywaĆ na naruszenie zabezpieczeŃ tych danych.
2. O naruszeniu ochrony danych osobowych mogĄŚwiadczyĆ następujĄce symptomy:
    - brak możliwoŚci uruchomienia przez użytkownika aplikacji pozwalajĄcej na dostęp do danych osobowych,
    - brak możliwoŚci zalogowania się do aplikacji,
    - ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika aplikacji lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
    - wyglĄd aplikacji inny niż normalny,
    - inny zakres danych niż normalnie dostępny dla użytkownika,
    - znaczne spowolnienie działania systemu informatycznego,
    - pojawienie się niestandardowych komunikatów generowanych przez system informatyczny,
    - Ślady włamania lub prób włamania do obszaru, w którym przetwarzane sĄ dane osobowe,
    - Ślady włamania lub prób włamania do pomieszczeŃ, w których odbywa się przetwarzanie danych osobowych, w szczególnoŚci do serwerowni oraz do pomieszczeŃ, w których przechowywane sĄnoŚniki kopii awaryjnych,
    - włamanie lub próby włamania do szafek, w których przechowywane sĄ w postaci elektronicznej lub papierowej ï noŚniki danych osobowych,
    - zagubienie lub kradzież noŚnika danych,
    - kradzież sprzętu informatycznego, w którym przechowywane były dane osobowe,

- informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,
- fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia siły wyższej,
- podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

3. Każdy pracownik Urzędu biorący udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialny za bezpieczeństwo tych danych.
    - w szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogących spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania ABI lub innej osoby wskazanej przez niego,
    - osoba zatrudniona w Urzędzie, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym, powinna niezwłocznie poinformować o tym ABI lub osobę zatrudnioną przy przetwarzaniu danych, albo inną osobę upoważnioną przez niego,
    - ABI jest odpowiedzialny jest odpowiedzialny za przygotowanie i opublikowanie wykazu osób przez niego upoważnionych,
    - w przypadku niemożliwości zawiadomienia ABI lub osób przez niego upoważnionych, pracownik powinien powiadomić bezpośredniego przełożonego.
4. Informacja o pojawieniu się zagrożenia lub wystąpieniu zagrożenia danych osobowych:
    - informacja przekazywana jest przez pracownika osobiście lub telefonicznie,
    - informacja o której mowa w w/w podpunkcie powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia,
    - w przypadku, gdy zgłoszenie o podejrzeniu zaistniałego incydentu otrzyma inna osoba niż ABI, jest ona obowiązana poinformować o tym ABI,
    - pracownik może zostać poproszony przez ABI o potwierdzenie zauważonego faktu na piśmie.
5. Czynności pierwszej reakcji użytkownika stwierdzającego naruszenie.
    1) Do czasu przybycia ABI lub upoważnionej przez niego osoby, zgłaszający:

- niezwłocznie podejmuje czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnia w działaniu również ustalenie przyczyn lub sprawców,
- zabezpiecza dostęp do miejsca lub urządzenia przez osoby trzecie,
- wstrzymuje prace na komputerze na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, których funkcjonowanie w związku z naruszeniem ochrony zostało wstrzymane,
- nie zmienia położenia przedmiotów, które pozwalają stwierdzić naruszenie ochrony lub odtworzyć jej okoliczności,
- podejmuje, stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
- wstępnie udokumentował zaistniałe naruszenie.

2) Dokonywanie zmian w miejscu naruszenia ochrony jest dopuszczalne, jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia groźącemu niebezpieczeństwu.

6. ABI niezwłocznie po uzyskaniu sygnału o naruszeniu danych osobowych powinien:
   - zapoznać się z zaistniałą sytuacją i dokonać wyboru metody dalszego postępowania pracy Urzędu,
   - zapisać wszelkie informacje związane z danym zdarzeniem,
   - na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,
   - przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,
   - dokonać fizycznego odgłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nieuprawnionej,
   - wylogować użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
   - dokonać zmiany hasła na konto ABI i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,
   - zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,

- rozważył możliwość i potrzebę powiadomienia o zaistniałym naruszeniu ADO,
- nawiązał bezpośredni kontakt, jeśli zachodzi taka potrzeba, ze specjalistami spoza Urzędu,
- zamknął i opieczętował urządzenia, w których przechowywane są dane osobowe w formie cyfrowej.

7. ABI podejmuje działania zmierzające do wyjaśnienia zgłoszonego zdarzenia. W szczególności może on dokonywać, w zależności od zgłoszonego zdarzenia:
    - wizji lokalnej w zakresie adekwatnym do rodzaju zgłoszonego zdarzenia,
    - przeprowadzenia wywiadów z pracownikami w celu ustalenia zaistniałych faktów,
    - Przeprowadzenia analizy poprawności funkcjonowania systemu informatycznego, jeżeli zgłoszone zdarzenie było związane z nieprawidłowym jego funkcjonowaniem,
    - przeprowadzenia analizy zapisu zdarzeń w systemie informatycznym z uwzględnieniem zapisu operacji realizowanych przez użytkowników,
    - przeprowadzenia analizy danych przetwarzanych w systemie informatycznym, jeżeli zgłoszone zdarzenie mogło być spowodowane utratą dostępności lub integralności przetwarzania danych,
    - zabezpieczenia danych przetwarzanych w systemie informatycznym dotkniętym incydentem, w szczególności danych konfiguracyjnych tego systemu,
    - zebranie innych materiałów pozwalających na wyjaśnienie przyczyn zaistnienia incydentu, jego charakteru i potencjalnych skutków.

8. Czynności pierwszej reakcji ASI

ASI przystępuje do usuwania skutków incydentu i przywrócenia prawidłowego przebiegu procesu przetwarzania danych osobowych. W szczególności działania związane z usuwaniem skutków incydentu mogą obejmować:

- przeprowadzenie naprawy sprzętu informatycznego,
- rekonfigurację sprzętu informatycznego,
- wprowadzenie poprawek do oprogramowania,
- rekonfigurację oprogramowania,
- odtworzenie danych z kopii awaryjnych,
- modyfikację danych w celu odtworzenia ich integralności,

- wycofanie z użycia materiału kryptograficznego,
- inne naprawy urządzeń wchodzących w skład infrastruktury informatycznej wspomagających lub zabezpieczających działanie.

9. ABI i ASI mogą odstąpić od skutków usuwania incydentu, jeżeli został on spowodowany działaniem celowym, a całkowite wyjaśnienie zdarzenia i wyciągnięcie konsekwencji wobec sprawców jest istotniejsze niż przerwa w działaniu systemu. Istniejący stan systemu informatycznego jest niezmieniony w celach dowodowych do czasu wyjaśnienia sprawy.
10. Przy usuwaniu skutków incydentu z wykorzystaniem odtwarzania danych z kopii awaryjnych ASI zobowiązany jest upewnić się, że odtworzone dane zostały zapisane przed wystąpieniem incydentu i w szczególności dotyczy to przypadków odtwarzania systemu po infekcji wirusowej.
11. Osoby upoważnione:
    - w sytuacjach wyjątkowych wszystkie powyżej opisane działania związane z usuwaniem skutków incydentu i wyjaśnianiem jego przyczyn mogą być realizowane przez osoby upoważnione przez ABI,
    - ABI odpowiada za sporządzenie listy pracowników mających prawo do podejmowania odpowiednich kroków w razie wystąpienia incydentu w sytuacji, gdy nie mogą one być wykonane osobiście przez niego.
12. Raporty i powiadomienia:
    - ABI określa, na podstawie przeprowadzonych wyjaśnień, przyczyny zaistnienia incydentu,
    - jeżeli incydent był spowodowany celowym działaniem, ABI jest zobowiązany do pisemnego powiadomienia Burmistrza Miasta i Administratora Danych,
    - Burmistrz Miasta i Administrator Danych, biorąc pod uwagę charakter zdarzenia, może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w urządzie.
13. Czynności końcowe:
    - ABI dokumentuje w raporcie, każdy zaistniały przypadek naruszenia ochrony danych osobowych,
    - dokumentacja, o której mowa powyżej, obejmuje następujące informacje:
      - imię i nazwisko osoby zgłaszającej incydent,

- imiń i nazwisko osoby przyjmujĄcej zgğoszeni incydentu,
- okreŚlenie czasu i miejsca incydentu,
- opis zgğoszonego incydentu,
- przyczyn wystĄpienia naruszenia,
- opis podjńtych działaŒ naprawczych,
- wyniki przeprowadzonego badania wyjaŚniajĄcego,
- ocenń skutecznoŚci przeprowadzonego postńpowania naprawczego,
- podjńte Środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszğoŚci naruszenia ochrony danych osobowych.

14. CzynnoŚci koŒcowe i analiza.

ABI i ASI w oparciu o posiadanĄ dokumentacjń, odpowiedzialni sĄ za przeprowadzanie przynajmniej raz w roku analizy zaistniağych incydentów w celu:

- okreŚlenia skutecznoŚci podejmowanych działaŒ wyjaŚniajĄcych i naprawczych,
- okreŚlenia wymagaŒ działaŒ zwińkszajĄcych bezpieczeŒstwo systemu informatycznego i minimalizujĄcych ryzyko zaistnienia incydentów,
- okreŚlenia potrzeb z zakresie szkoleŒ uŻytkowników systemu informatycznego przetwarzajĄcego dane osobowe.

Rozdział VIII
Postanowienia końcowe

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
2. ABI zobowiązany jest prowadzić ewidencje osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego **załącznik nr 9** do niniejszego dokumentu.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym ABI.
4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia ABI nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 poz. 1182 i 1662)
5. W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 poz. 1182 i 1662), 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) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji i do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz.U. z 2004 r. Nr. 100, poz. 1024).
6. Niniejsza polityka bezpieczeństwa w Urzędzie wchodzi w życie z dniem jej podpisania przez Burmistrza Miasta Zawidowa.