ZARZĄDZENIE NR 45
WÓJTA GMINY SIENNO

z dnia 14 października 2013 r.

w sprawie zatwierdzenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych w Urzędzie Gminy Sienno

Na podstawie **§ 3** Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) zarządza się, co następuje:

§ 1. 1. Zatwierdza się „Politykę bezpieczeństwa przetwarzania danych osobowych" stanowiącą załącznik nr 1 do zarządzenia.

2. Zatwierdza się „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" stanowiącą załącznik nr 2 do zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Administratorowi bezpieczeństwa informacji.

§ 3. Zarządzenie wchodzi w życie z dniem 1 listopada 2013 r.

Załącznik Nr 1 do Zarządzenia Nr 45

Wójta Gminy Sienno

z dnia 14 października 2013 r.

Polityka bezpieczeństwa przetwarzania danych osobowych

Mając na względzie właściwe wykonywanie obowiązków administratora danych, określonych ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych w celu zapewnienia ochrony przetwarzanych danych osobowych, wdraża się „Politykę bezpieczeństwa przetwarzania danych osobowych" (zwaną dalej „Polityką bezpieczeństwa") zgodnie z wymogami Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

I. Postanowienia ogólne.

Ilekroć w polityce bezpieczeństwa jest mowa o:

1/ ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;

2/ rozporządzeniu – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 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/ administratorze danych osobowych /w skrócie AD/– rozumie się przez to Gminę Sienno w imieniu, której działa Wójt Gminy;

4/ administratorze bezpieczeństwa informacji /w skrócie ABI /– rozumie się przez to pracownika wyznaczonego na to stanowisko będącego jednocześnie administratorem systemów informatycznych /w skrócie ASI/;

5/ osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych;

6/ użytkowniku – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznane hasło;

7/ przetwarzającym – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawartej zgodnie z art. 31 ustawy;

8/ odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

a/osoby, której dane dotyczącą,

b/osoby upoważnionej do przetwarzania danych,

c/przedstawiciela, o którym mowa w art. 31a ustawy,

d/organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

e/podmiotu, o którym mowa w art. 31 ustawy,

9/ identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

10/ haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

11/ sieci telekomunikacyjnej – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 32 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne;

12/ sieci publicznej – rozumie się przez to publiczną sieć telekomunikacyjną w rozumieniu art.2 pkt 29 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne;

13/ teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

14/ rozliczalności – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

15/ integralność danych - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

16/ poufność danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

17/ raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

18/ uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Cele polityki bezpieczeństwa:

1. Wdrożenie polityki bezpieczeństwa ma na celu zabezpieczenie przetwarzania danych osobowych w systemach informatycznych i kartotecznych.

2. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa w rozumieniu § 6 rozporządzenia w związku z tym, że w zbiorach danych AD przetwarzane są również dane drażliwe a sieć lokalna posiada dostęp do sieci publicznej.

3. Niniejszy dokument opisuje zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia niezbędnych do uzyskania tego bezpieczeństwa.

Zakres stosowania polityki.

1. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w systemach informatycznych oraz w sposób tradycyjny w księgach i wykazach i innych zbiorach ewidencyjnych.

2. Procedury i zasady określone w niniejszym dokumencie mają zastosowanie wobec osób upoważnionych do przetwarzania danych osobowych zatrudnionych lub świadczących usługi na podstawie umów o pracę, umów zlecenia, umów o dzieło, umów kontraktowych oraz stażystów, praktykantów itp.

II. Organizacja przetwarzania danych osobowych.

Administrator danych osobowy – AD realizuje zadania w zakresie ochrony danych osobowych, w tym w szczególności:

1/ wyznacza ABI i ASI;

2/ upoważnia osoby do przetwarzania danych osobowych w określonym przez ABI zakresie;

3/ podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpieczeństwa przetwarzania danych osobowych;

4/ zleca sekretarzowi gminy, aby zapewnił użytkownikom odpowiednie wyposażenie i organizację stanowisk pracy umożliwiające bezpieczne przetwarzanie danych;

5/ podejmuje decyzje o celach i środkach przetwarzania danych osobowych zwłaszcza z uwzględnieniem zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych.

Administrator bezpieczeństwa informacji – ABI - zadania:

1/ odpowiada za wdrożenie stosownych środków organizacyjnych, technicznych i fizycznych w celu zapewnienia bezpieczeństwa danych osobowych;

2/ sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń;

3/ nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom;

4/ dokonuje zgłoszeń zbioru danych do rejestracji w GIODO i aktualizacji oraz zgłasza zbiory do wkreślenia;

5/ zatwierdza wzory dokumentów /odpowiednie klauzule w dokumentach dotyczących ochrony danych osobowych przygotowane przez pracowników urzędu Gminy;

6/ prowadzi ewidencje i inną dokumentację z zakresu ochrony danych osobowych;

7/ prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych;

8/ podejmuje odpowiednie działania w wypadku naruszenia lub podejrzenia naruszenia systemu informatycznego;

9/ przygotowuje i prowadzi szkolenia szkoleniowe z zakresu ochrony danych osobowych dla osób upoważnionych do przetwarzania danych osobowych;

10/ prowadzi ewidencję osób upoważnionych do przetwarzania danych;

11/ występuje z wnioskiem do AD o przyznanie upoważnienia do przetwarzania danych osobowych;

12/ występuje z wnioskiem o odwołanie upoważnienia do przetwarzania danych osobowych oraz do wyrejestrowania użytkownika z systemu informatycznego;

13/ nadaje identyfikator i hasła osobie upoważnionej do przetwarzania danych osobowych.

Administrator systemu informatycznego – ASI - zadania:

1/ zarządza systemem informatycznym, w którym przetwarzane są dane osobowe posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;

2/ przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym są przetwarzane dane osobowe;

3/ przydziela każdemu użytkownikowi identyfikator i hasło do systemu informatycznego oraz modyfikuje uprawnienia;

4/ nadzoruje działanie mechanizmów uwierzytelnienia użytkowników oraz kontroli dostępu do danych osobowych;

5/ podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu Informatycznego;

6/ wyrejestrowuje użytkowników;

7/ zmienia w poszczególnych stacjach roboczych hasła dostępu ujawniając je wyłącznie danemu użytkownikowi oraz w razie potrzeby ABI lub AD;

8/ w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ABI o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia;

9/ prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;

10/ nadzoruje wykonywanie napraw, konserwacji oraz likwidację urządzeń komputerowych, na których zapisane są dane osobowe, sprawuje nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych;

11/ podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej eletransmisji.

Upoważnienie do przetwarzania danych osobowych.

1. Użytkownik może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez AD i tylko w celu wykonywania nałożonych na niego obowiązków.

2. Rozwiązanie stosunku pracy w tym odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.

3. Użytkownicy danych składają pisemne oświadczenie, że zobowiązują się do zachowania tajemnicy danych osobowych oraz przestrzegania procedur ich bezpiecznego przetwarzania.

4. Zakaz udostępniania danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych a także po ustaniu stosunku pracy lub odwołania z pełnionej funkcji.

5. Naruszenie przez użytkowników danych osobowych procedur bezpieczeństwa przetwarzania tych danych, w szczególności świadome udostępnienie danych osobie nieupoważnionej, jest ciężkim naruszeniem obowiązków pracowniczych.

6. Użytkownicy danych zobowiązani są do:

1/ zapoznania się z przepisami prawa w zakresie ochrony danych osobowych, w tym przepisami niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

2/ stosowania określonych przez AD oraz ABI procedur oraz instrukcji mających na celu zgodne z prawem przetwarzanie danych;

3/ stosowanie zabezpieczeń danych przed ich udostępnianiem osobom nieupoważnionym.

III. Infrastruktura przetwarzania danych osobowych.

1. Obszar przetwarzania danych osobowych obejmuje siedzibę urzędu Gminy i szczegółowo jest opisany w załączniku nr 1 do polityki.

2. Zbiory danych osobowych przetwarzanych określa wykaz stanowiący załącznik nr 2 do polityki.

3. Strukturę zbiorów danych opisano w załączniku nr 3 do polityki.

4. Sposób przepływu danych pomiędzy poszczególnymi systemami opisano w załączniku nr 4 do polityki.

IV. Strategia zabezpieczenia danych osobowych /działania niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzania danych/.

Bezpieczeństwo osobowe.

AD każdemu pracownikowi, którego zamierza upoważnić do przetwarzania danych osobowych nadaje upoważnienie do dostępu do informacji niejawnych o klauzuli „zastrzeżone".

Strefy bezpieczeństwa.

1. W urzędzie gminy wydzielono strefy bezpieczeństwa „klasy I" i „klasy II".

2. Strefa bezpieczeństwa „klasy I" obejmuje pomieszczenie z serwerami – mogą w niej przebywać wyłącznie pracownicy posiadający stosowne upoważnienie a osoby postronne w ogólne nie mają dostępu.

3. Strefa bezpieczeństwa „klasy II" obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie administratora danych zgodnie z załącznikiem nr 1 – osoby postronne mogą w niej przebywać tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych.

Zabezpieczenie sprzętu.

1. Serwery zlokalizowane są w odrębnym pomieszczeniu zamykanym na drzwi z dwoma zamkami patentowymi, oknem zabezpieczonym kratą oraz systemem alarmowym – pokój nr 12.

2. Wszystkie komputery i monitory systemu informatycznego są zasilane za pośrednictwem zasilaczy awaryjnych tzw. UPS-ów.

3. Bieżącą konserwację i naprawy urządzeń systemu informatycznego wykonują upoważnieni pracownicy urzędu gminy w obecności ABI.

4. Naprawy mogą być wykonywane przez firmy i osoby zewnętrzne w siedzibie AD po zawarciu umowy o powierzenie przetwarzania danych osobowych.

5. ABI prowadzi ewidencję awarii, prac konserwacyjnych i napraw systemu informatycznego.

6. Nie dopuszcza się konserwacji i napraw sprzętu poza siedzibą AD.

7. Sprzęt służący do przetwarzania danych osobowych przeznaczony do wycofania z użytkowania może być przekazany do utylizacji lub zbywany tylko po fizycznym usunięciu nośnika danych.

8. ABI poucza użytkowników jak postępować aby:

a/zapewnić ochronę nośników elektromagnetycznych danych a w szczególności nośników, na których są przechowywane kopie zapasowe,

b/zapewnić prawidłową lokalizację komputerów i monitorów.

Zabezpieczenia we własnym zakresie.

ABI prowadzi działania mające na celu stosowanie przez pracowników poniższych zaleceń:

1/ nieujawniania informacji o danych osobowych osobom nieuprawnionym;

2/ kasowania danych na nośnikach przenośnych po ich wykorzystaniu;

3/ niepozostawiania bez kontroli dokumentów, płyt CD, komputerów przenośnych itd.;

4/ ustawianie ekranów komputerowych tak, aby utrudnić odczyt danych przez osoby postronne;

5/ dbania o wentylację i czystość komputerów;

6/ powstrzymywania się od samodzielnej ingerencji w oprogramowanie i konfigurację sprzętu;

7/ przestrzegania swoich uprawnień w systemie;

8/ niepozostawianie osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej;

9/ opuszczanie stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub zablokowaniu stacji roboczej w inny sposób;

10/ zakazu robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków pracownika: jednostkowe dane mogą być kopiowane na nośniki magnetyczne optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach, po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki na których są przechowywane;

11/ nieudostępniania niezaszyfrowanych danych osobowych pocztą elektroniczną;

12/ niewynoszenia poza urząd gminy zbiorów danych na jakichkolwiek nośnikach;

13/ wykonywania kopii roboczych danych, na których się właśnie pracuje tak często aby zapobiec ich utracie;

15/ kończenia pracy na stacji roboczej poprzez prawidłowe wylogowanie się użytkownika, wyłączenie komputera oraz odcięci zasilania w UPS;

16/ niszczenia w niszczarce lub chowanie do szaf zamykanych na klucz wszelkich roboczych wydruków zawierających dane osobowe po zakończeniu pracy;

17/ chowanie do zamykanych na klucz szaf akt z danymi osobowymi po zakończeniu pracy;

18/ umieszczenia kluczy do szaf w ustalonym miejscu;

19/ zamykania drzwi pomieszczeń na klucz po zakończeniu dnia pracy.

Postępowanie z nośnikami i ich bezpieczeństwo.

Osoby przetwarzające dane osobowych przy wykorzystywaniu nośników przenośnych winne przestrzegać poniższych wymagań:

1/ dane z nośników /płyty CD, pamięci usb itp./ po wprowadzeniu ich do systemu informatycznego są trwale usuwane z tych nośników poprzez fizyczne zniszczenie lub skasowanie danych;

2/ w przypadku uzasadnionej potrzeby dane osobowe jednostkowe mogą być przechowywane na specjalnie oznaczonych nośnikach: nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nie mogą być udostępniane osobom postronnym, po ustaniu przydatności tych danych nośniki powinny być trwale zniszczone;

3/ nośniki przed ich przekazaniem do utylizacji należy fizycznie zniszczyć;

4/ po wykorzystaniu wydruki zawierające dane osobowe należy niezwłocznie zniszczyć w niszczarce;

5/ zabrania się wynoszenia poza Urząd Gminy bez zezwolenia ABI nośników z danymi osobowymi.

Wymiana danych i ich bezpieczeństwo.

1. Komputery mające dostęp do sieci publicznej /Internetu/ zabezpiecza się odpowiednimi metodami i środkami.

2. ABI dobiera elektroniczne środki ochrony przed atakami z sieci publicznej stosownie do pojawiania się nowych zagrożeń /wirusy, robaki, trojany/ a także stosownie do rozbudowy systemu informatycznego i powiększania bazy danych.

3. Inne wymogi bezpieczeństwa systemów określają:

a/ instrukcje obsługi producentów sprzętu i używanych programów,

b/ wskazówki ABI,

c/„Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”.

Kontrola dostępu do systemu.

1. ABI każdej osobie upoważnionej do przetwarzania danych osobowych zakłada konto w systemie informatycznym opatrzone niepowtarzalnym identyfikatorem umożliwiające dostęp do danych zgodnie z zakresem upoważnienia do przetwarzania danych osobowych.

2. ABI przydziela upoważnionym pracownikom konto w systemie informatycznym dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem. System wymusza zmianę hasła przy pierwszym logowaniu.

3. ABI może w razie potrzeby przydzielić konto opatrzone identyfikatorem osobie upoważnionej do przetwarzania danych osobowych nie będącej pracownikiem urzęduj gminy.

4. ABI przydziela pierwsze hasło wymagane do uwierzytelnienia się w systemie po odebraniu od osoby upoważnionej do przetwarzania danych osobowych oświadczenia o zachowaniu w tajemnicy pierwszego i następnych haseł.

5. Dla zagwarantowania poufności i integralności przetwarzanych w systemiedanych osobowych konieczne jest przestrzeganie przez użytkowników swoichuprawnień tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasło oraz stosowania się do zaleceń ABI.

Kontrola dostępu do sieci lokalnej i publicznej.

1. System informatyczny posiada połączenie z siecią publiczną.

2. ABI może dokonywać zmian ustawień stacji roboczych w celu umożliwienia lub nie dostępu do Internetu.

Komputery przenośne i praca na odległość.

1. Zabrania się prowadzenia zbiorów danych osobowych i przetwarzania danych osobowych na komputerach przenośnych i nośnikach.

2. Komputery przenośne oraz nośniki danych wynoszone z urzędu Gminy nie mogą zawierać danych osobowych.

3. W zakresie nieuregulowanym w polityce bezpieczeństwa do pracy z wykorzystaniem komputerów przenośnych stosuje się postanowienia „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”.

Monitorowanie dostępu do systemu i jego użycia.

1. Systemy informatyczne rejestrują każde zalogowanie do systemu ze stacji roboczych.

2. Systemy posiadają funkcjonalność zapewniającą odnotowanie:

1/ daty pierwszego wprowadzenia danych do systemu;

2/ identyfikatora użytkownika wprowadzającego dane osobowe do systemu;

3/ źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą;

4 /informacji o odbiorcach danych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia;

5/ sprzeciwu wobec przetwarzania danych osobowych, o którym mowa w art. 32 ust.1 pkt 8 ustawy.

3. Odnotowanie informacji, o których mowa w pkt 1 i 2 następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzania danych.

4. ABI przeprowadza synchronizację zegarów stacji roboczej z serwerem ograniczając dopuszczalność zmian w ustawieniach zegarów.

5. Zmiany ustawień zegarów mogą być dokonywane jedynie przez ABI.

6. System informatyczny umożliwia zapisywanie zdarzeń wyjątkowych na potrzeby audytu i przechowywanie informacji o nich przez określony czas.

7. Zapisy takie obejmują:

1/ identyfikator użytkownika;

2/ datę i czas w zalogowania i wylosowania się z systemu;

3/ tożsamość stacji roboczej;

4/ zapisy udanych i nieudanych prób dostępu do systemu.

Przeglądy okresowe zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych.

1. ABI przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania.

2. ABI może przeprowadzić dodatkowe przeglądy w przypadku:

1/ zmian w obowiązującym prawie;

2/ zmian organizacyjnych.

3. Z przeglądu danych osobowych należy sporządzić protokół podpisywany przez ABI i użytkownika.

Szkolenia osób upoważnionych do przetwarzania danych.

1. ABI przygotowuje i prowadzi szkolenia w zakresie ochrony danych osobowych.

2. Obowiązkowe szkolenia przeprowadza się wobec:

1/ osoby, która ma zostać upoważniona do przetwarzania danych osobowych;

2/ wszystkich osób upoważnionych do przetwarzania danych osobowych w wypadku każdej zmiany zasad lub procedur ochrony danych osobowych;

3. Tematyka szkoleń obejmuje:

1/ przepisy i instrukcje dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach;

2/ sposoby ochrony danych osobowych przed osobami postronnymi i procedury udostępniania danych osobą, których one dotyczą;

3 /obowiązki osób upoważnionych do przetwarzania danych;

4/ zasady i procedury określone w polityce bezpieczeństwa.

Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych.

Naruszanie zasad określonych w polityce bezpieczeństwa przetwarzania danych osobowych, naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być traktowane jako ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym, w szczególności wynikającym z art. 51 i 52 ustawy oraz art. 266 KK.

V. Przegląd polityki bezpieczeństwa i audyty systemu.

1. Polityka bezpieczeństwa poddawana jest ocenie przynajmniej raz na rok.

2. W razie istotnych zmian dotyczących przetwarzania danych ABI może zarządzić ocenę polityki bezpieczeństwa stosownie do potrzeb.

3. ABI analizuje czy polityka bezpieczeństwa i pozostała dokumentacja jest adekwatna do zmian:

1/w budowie systemu informatycznego;

2/organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych;

3/ w obowiązującym stanie prawnym.

4. ABI po uzgodnieniu z Wójtem może, przeprowadzić audyt systemu.

5. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym przez ABI i pracownika.

VI. Postanowienia końcowe.

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie o znajomość jego treści.

.

załącznik nr 1

Wykaz

pomieszczeni tworzących obszar, w którym są przetwarzane dane osobowe

w budynku administracyjnym Sienno ul. Rynek 36/40 I piętro

Lp.	Miejsce przetwarzania numer pokoju	Zabezpieczenie pomieszczenia
1.	1	drzwi z zamkiem alarm
2.	2	drzwi z zamkiem alarm
3.	6	drzwi z zamkiem alarm
4.	9	drzwi z zamkiem alarm
5.	10	drzwi z zamkiem alarm
6.	12	drzwi z zamkiem alarm
7.	14	drzwi z zamkiem alarm
8.	16	drzwi z zamkiem alarm
9.	17	drzwi z zamkiem alarm
10.	21	drzwi z zamkiem alarm
11.	22	drzwi z zamkiem alarm

załącznik nr 2

Wykaz

zbiorów danych osobowych wraz ze wskazaniem programów

zastosowanych do przetwarzania tych danych

Lp.	Nazwa zbioru danych osobowych	Programy zastosowane do przetwarzania danych
1.	Rejestr podatników podatków gruntowych	Xpertis podatek rolny, leśny i od nieruchomości - Macrologic
2	Rejestr podatników podatku od środków transportowych	Xpertis podatek od środków transportowych- Macrologic
3	Kadry i płace	Xpertis Kadry i płace- Macrologic
4	Odpady komunalne	Xpertis odpady komunalne - Macrologic
5	Podatek akcyzowy - zwrot producentom	APAR - Cuprimex sp. Z o.o.
6	System bankowy	home banking - BS Iłża
7	Ewidencja ludności	SELWIN - Sygnity
8	Ewidencja dowodów osobistych	SOO - MSW
9	Akty stanu cywilnego	PB_USC - Technika sp. Z o.o.
10	Świadczenia rodzinne	SR - Sygnity
11	Fundusz alimentacyjny	FA - Sygnity
12	Pomoc materialna dla uczniów	ST - Sygnity
13	Rejestr zezwoleń na sprzedaż napojów alkoholowych	kartoteczny
14	Dodatki mieszkaniowe	kartoteczny
15	Zaliczka alimentacyjna	kartoteczny

Załącznik nr 3

Sposób

przepływu danych pomiędzy różnymi systemami informatycznymi

Lp.	Nazwa zbioru danych osobowych	Sposób przepływu
1.	Rejestr podatników podatków gruntowych	Brak przepływu
2	Rejestr podatników podatku od środków transportowych	Brak przepływu
3	Podatek akcyzowy - zwrot producentom	Sieć wewnętrzna
4	Odpady komunalne	Brak przepływu
5	Kadry i płace	Sieć wewnętrzna
6	System bankowy	Sieć wewnętrzna
7	Ewidencja ludności	Brak przepływu
8	Ewidencja dowodów osobistych	Brak przepływu
9	Urząd stanu cywilnego	Brak przepływu
10	Świadczenia rodzinne	Sieć wewnętrzna
11	Fundusz alimentacyjny	Sieć wewnętrzna
12	Pomoc materialna dla uczniów	Brak przepływu

Załącznik Nr 4

Struktura zbiorów danych osobowych

Lp.	Nazwa zbioru danych osobowych	Zawartość poszczególnych pól informacyjnych i powiązania między nimi
1.	Rejestr podatników podatków gruntowych	imię i nazwisko podatnika, jego adres zamieszkania, PESEL, NIP, imiona rodziców
2	Rejestr podatników podatku od środków transportowych	imię i nazwisko podatnika, jego adres zamieszkania, PESEL, NIP, imiona rodziców
3	Podatek akcyzowy - zwrot producentom	imię i nazwisko podatnika, jego adres zamieszkania, PESEL, NIP, imiona rodziców
4	Odpady komunalne	imię i nazwisko podatnika, jego adres zamieszkania, PESEL,
5	Kadry i płace	imię i nazwisko danej osoby, jej adres, numer telefonu, wysokość wynagrodzenia, wykształcenie, urlopy, numer dowodu osobistego, numer PESEL, NIP, imiona rodziców, data i miejsce urodzenia i numer konta bankowego informacje o urlopach i zwolnieniach lekarskich, dokładne dane o wykształceniu, o odbytych szkoleniach, informacje o posiadanych dzieciach, zawartych związkach małżeńskich, dane o niekaralności z KRK, dane o stanie zdrowia.
6	System bankowy	imię i nazwisko, numer konta i nazwę banku.
7	Ewidencja ludności	imię i nazwisko, nazwisko rodowe, datę i miejsce urodzenia, miejsce zamieszkania, PESEL, nr dowodu osobistego, stan cywilny
8	Ewidencja dowodów osobistych	imiona i nazwisko, nazwisko rodowe, datę i miejsce urodzenia, miejsce zamieszkania, PESEL, nr dowodu osobistego, kolor oczu, wzrost
9	Urząd stanu cywilnego	imiona i nazwiska, daty i miejsca urodzenia, miejsce zamieszkania, PESEL , stan cywilny, wykształcenie, zawód
10	Świadczenia rodzinne	imię i nazwiska adres zamieszkania, PESEL, NIP, imiona rodziców, zawartych związkach małżeńskich, dane o niepełnosprawności
11	Fundusz alimentacyjny	imię i nazwiska adres zamieszkania, PESEL, NIP, imiona rodziców, zawartych związkach małżeńskich, dane o niepełnosprawności.
12	Pomoc materialna dla uczniów	imię i nazwiska adres zamieszkania, PESEL, NIP, imiona rodziców, zawartych związkach małżeńskich, dane o niepełnosprawności.
13	Rejestr zezwoleń na sprzedaż napojów alkoholowych	imię i nazwiska adres zamieszkania, PESEL, NIP
14	Dodatki mieszkaniowe	imię i nazwiska jego adres zamieszkania, PESEL, NIP, imiona rodziców, zawartych związkach małżeńskich,
15	Zaliczka alimentacyjna	imię i nazwiska jego adres zamieszkania, PESEL, NIP, imiona rodziców, zawartych związkach małżeńskich, dane o niepełnosprawności.

Załącznik Nr 2 do Zarządzenia Nr 45

Wójta Gminy Sienno

z dnia 14 października 2013 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

I. Cel instrukcji

Instrukcja określa sposób zarządzania systemami informatycznymi wykorzystywanymi do przetwarzania danych osobowych przez administratora danych w celu zabezpieczenia danych osobowych przed zagrożeniami w tym zwłaszcza przed ich udostępnieniem osobowym nieuprawnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

II. Definicje.

Ilekroć mowa jest w instrukcji o:

1/ ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;

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;

3/ administratorze danych – rozumie się przez to gminę reprezentowaną przez wójta gminy;

4/ administratorze bezpieczeństwa informacji – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji - ABI będącą jednocześnie administratorem systemu informatycznego – ABS;

5/ osobie upoważnionej do przetwarzania danych osobowych – rozumie się prze to osobę zatrudnioną na podstawie umowy o pracę, umowy zlecenia, lub innej umowy, której wydane zostało przez administratora danych upoważnienie do przetwarzania danych osobowych;

6/ użytkowniku – rozumie się prze to osobę upoważnioną do przetwarzania danych osobowych, której nadano uprawnienia do przetwarzania danych w systemie informatycznym;

7/ systemie informatycznym administratora danych – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych: w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych;

8/ identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w wyznaczonym przez administratora danych osobowych obszarach systemu informatycznego;

9/ haśle – rozumie się przez to ciąg znaków literowych, cyfrowych, zawierających duże i małe litery oraz znaki specjalne, znany jedynie osobie, której nadano identyfikator użytkownika;

10/ odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

a/ osoby, której dane dotyczą,

b/ przedstawiciela, o którym mowa w art. 31a ustawy,

c/ podmiotu, o którym mowa w art. 31 ustawy,

d/ organów administracji publicznej, którym dane są udostępnianie w związku z prowadzonym postępowaniem.

11/ serwisancie – rozumie się prze to firmę lub pracownika firmy zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego oraz systemów informatycznych;

III. Poziom bezpieczeństwa

Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa przetwarzania w systemie informatycznym połączonym z siecią publiczną, wprowadza się „poziom wysoki bezpieczeństwa w rozumieniu § 6 rozporządzenia.

IV. Nadawanie i rejestrowanie /wyrejestrowanie/ uprawnień do przetwarzania danych w systemie informatycznym.

1. Dostęp do systemu służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych zarejestrowana jako użytkownik przez ABI.

2. Rejestracja użytkownika polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

V. Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Identyfikator składa się z sześciu znaków, z których dwa pierwsze odpowiadają dwóm pierwszym literom imienia użytkownika, a cztery kolejne odpowiadają czterem pierwszym literom jego nazwiska. W identyfikatorze pomija się polskie znaki diakrytyczne.

2. W wypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika nadaje się inny identyfikator odstępując od zasady określonej w pkt 1.

3. Hasło powinno składać się z niepowtarzalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry i znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani z jego imieniem lub nazwiskiem.

4. System informatyczny musi zawierać opcję zmiany hasła co 30 dni. ABI może w uzasadnionych sytuacjach może polecić dokonanie zmiany hasła.

5. Zabrania się udostępniania swojego identyfikatora i hasła innym osobom oraz wykorzystywania identyfikatora lub hasła innego użytkownika.

6. Wyrejestrowanie użytkownika z systemu informatycznego dokonuje ABI.

7. Wyrejestrowanie z systemu może mieć charakter czasowy lub trwały.

8. Wyrejestrowanie następuje przez:

1/ zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę;

2/ usunięcie danych użytkownika z bazy użytkowników systemu.

9. Przyczyną czasowego wyrejestrowania użytkownika z systemu jest:

1/ nieobecność w pracy trwająca dłużej niż 30 dni;

2/ zawieszenie w pełnieniu obowiązków służbowych.

10. Przyczyną czasowego wyrejestrowania użytkownika z systemu może być:

1/ wypowiedzenie umowy o pracę;

2/ wszczęcie postępowania dyscyplinarnego.

11. Przyczyną trwałego wyrejestrowania użytkownika z systemu jest rozwiązanie umowy o pracę.

12. Hasło administratora systemu przechowuje się w metalowej szafie, do której mają dostęp wójt i sekretarz.

VI. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

A. Tryb pracy na poszczególnych stacjach roboczych.

1. Rozpoczęcie pracy na stacji roboczej następuje po włączeniu napięcia i uruchomienia komputera, wprowadzeniu hasła do systemu operacyjnego a następnie identyfikatora i hasła do oprogramowania.

2. W pomieszczeniu, w którym przetwarzane są dane osobowe mogą znajdować się inne osoby tylko w obecności użytkownika.

3. Monitory komputerowe należy chronić ustawiać w sposób uniemożliwiający ich podgląd przez interesantów.

4. Monitory winne wygaszać ekrany po maksymalnie 5 minutach od przerwania pracy na komputerze.

5. W przypadku opuszczenia stanowiska pracy użytkownik obowiązany jest aktywować wygaszacz ekranu lub w inny sposób zablokować stację roboczą.

6. Wprowadza się zakaz wykonywania kopii całych zbiorów danych. Całe zbiory danych mogą być kopiowane tylko przez administratora bezpieczeństwa informacji lub automatycznie przez system z zachowaniem procedur ochrony danych osobowych

7. Wypisy ze zbiorów danych udostępniane są na podstawie art. 29 ustawy.

8. Obowiązuje zakaz wynoszenia poza urząd zbiorów danych oraz obszernych jego wypisów nawet w postaci zaszyfrowanej.

9. Przetwarzając dane osobowe, należy odpowiedni często zapisywać dane, na których się właśnie pracuje, tak aby zapobiec ich utracie.

10. Zakończenie pracy na stacji roboczej następuje po zapisaniu danych, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera i odcięciu napięcia za zasilaczu awaryjnym.

11. Przed opuszczeniem pokoju należy:

1/ zniszczyć w niszczarce lub schować do szaf zamykanych wszelkie wykonane wydruki zawierające dane osobowe;

2/ schować do zamykanych na klucz wszelkie akta zawierające dane osobowe;

3/ schować klucz od szaf w ustalony sposób.

12. Opuszczając pokój należy zamknąć drzwi na klucz, jeżeli w urzędzie nie rozpoczęły pracy służby odpowiedzialne za sprzątanie.

B. Tryb pracy na komputerach przenośnych.

1. Zabrania się prowadzenia zbiorów danych osobowych i przetwarzania danych osobowych na komputerach przenośnych i nośnikach.

2. Komputery przenośne oraz nośniki danych wynoszone z urzędu gminy nie mogą zwierać danych osobowych

3. W zakresie nieuregulowanym w polityce bezpieczeństwa do pracy z wykorzystaniem komputerów przenośnych stosuje się postanowienia „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

VII. Procedury tworzenia kopii zapasowych zbiorów danych.

1. Kopie zapasowe zbiorów danych tworzy się nie rzadziej niż co dwa miesiące.

2. Każdą kopię tworzy się na oddzielnych nośnikach informatycznych.

4. ABI dokonuje okresowych przeglądów kopii zapasowych i ocenia ich przydatność do odtworzenia zasobów zbiorów.

5. ABI po stwierdzenie utraty przez kopie zapasowe waloru przydatności może dokonać ich zniszczenia.

6. Z procedury zniszczenia sporządza się protokół.

VIII. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe oraz ich kopii.

1. Zbiory danych przechowywane są dyskach twardych serwerów i stacji roboczych obsługującym systemy informatyczne.

2. Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną bez ich uprzedniego zaszyfrowania.

3. Na nośnikach, o których mowa w ust. 2 dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.

4. W przypadku posługiwania się nośnikami danych pochodzących od podmiotu zewnętrznego użytkownik jest zobowiązany jest do sprawdzenia go programem antywirusowym oraz do oznakowania tego nośnika.

5. Nośniki magnetyczne raz użyte do przetwarzania danych, których usunięto dane nie mogą być ponownie wykorzystane i podlegają ochronie w trybie niniejszej instrukcji.

6. Nośniki magnetyczne z zaszyfrowanymi jednostkowymi danymi osobowymi są – na czas ich użyteczności – przechowywane w zamkniętych na klucz szafach, a po ich wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki te są niszczone.

7. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych.

8. Kopie zapasowe przechowuje się w pomieszczeniach wyznaczonych w szafach metalowych.

9. ABI przeprowadza okresowo weryfikację przydatności sporządzonych kopii do ewentualnego odtworzenia danych.

10. Kopie zapasowe programów i kopie systemu informatycznego przechowywane są w ogniotrwałej szafie znajdującej się w innym pomieszczeniu niż serwer . Po wygaśnięciu przydatności tych kopii są one trwale kasowane lub nośniki je przechowujące są niszczone mechanicznie w niszczarce.

IX. Sposób zabezpieczenia systemu informatycznego przed szkodliwym oprogramowaniem, którego celem jest uzyskania nieuprawnionego dostępu do systemu informatycznego.

1. Sprawdzenie obecności szkodliwych oprogramowań systemie informatycznym oraz ich usuwanie odbywa się za pomocą licencjonowanego oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych.

2. Oprogramowanie, o którym mowa w ust. 1 sprawuje ciągły nadzór /ciągła praca w tle/ nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.

3. Niezależnie od ciągłego nadzoru ABI raz na 6 miesięcy przeprowadza kontrolę na obecności na serwerach i stacjach roboczych szkodliwych oprogramowań.

4. Do obowiązków ABI należy aktualizacja oprogramowania antywirusowego.

5. Użytkownik jest obowiązany zawiadomić ABI o pojawiających się komunikatach wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

6. Użytkownicy mogą korzystać z zewnętrznych nośników danych po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.

7. Dostęp do Internetu na stacjach roboczych jest możliwy tylko przy zastosowaniu zabezpieczeń typu firewall.

X. Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem

danych osobowych.

1. System informatyczny umożliwia automatycznie:

1/ przypisanie wprowadzanych danych użytkownikowi /identyfikatorowi użytkownika/, który te dane wprowadza do systemu;

2/ sygnalizacja wygaśnięcia czasu obowiązywania hasła dostępu do stacji roboczej;

3/ sporządzanie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie raportu zawierającego:

a/datę pierwszego wprowadzenia danych do systemu,

b identyfikator użytkownika wprowadzającego te dane,

c/źródła danych w przypadku zbierania danych nie od osoby, której one dotyczą,

d/informacje o odbiorcach danych, którym dane osobowe zostały udostępnione,

e/sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy,

2. Odnotowanie informacji, o których mowa w ust 1 pkt 3, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzania danych.

XI. Procedury wykonywania przeglądów konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1. Przeglądu i konserwacji systemu dokonuje ABI doraźnie.

2. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu /log systemowy/ administrator dokonuje raz na miesiąc.

3. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy udziale ABI raz na miesiąc.

4. Zapisy logów systemowych powinny być przeglądane przez administratora codziennie oraz każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.

5. Kontrole i testy przeprowadzane przez administratora powinny obejmować zarówno dostęp do zasobów systemu jak i profile oraz uprawnienia poszczególnych użytkowników.

XII. Naprawy urządzeń komputerowych z danymi osobowymi.

1. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym administratora danych przeprowadzać należy – jeżeli jest to możliwe- przez upoważnionych pracowników urzędu pod nadzorem administratora.

2. Naprawy urządzeń komputerowych i zmiany w systemie informatycznym przeprowadzane przez serwisanta pod nadzorem ABI, jeżeli jest to możliwe w siedzibie administratora danych.

3. Naprawy i zmiany w systemie informatycznym mogą być przeprowadzane poza siedzibą administratora danych po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych a jeśli byłoby to niecelowe to po podpisaniu umów powierzenia przetwarzania danych osobowych .

4. Jeżeli nośnik danych /dysk, płyta lub inny / zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych to należy go zniszczyć mechanicznie w niszczarce lub w inny sposób.

XIII. Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego.

1. Użytkownik zobowiązany jest zawiadomić ABI o każdym przypadku naruszenia lub o podejrzeniu naruszenia bezpieczeństwa systemu a w szczególności o:

1/ naruszenia hasła dostępu i identyfikatora /system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzania hasła/;

2/ częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień;

3/ braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera;

4/ wykrycia szkodliwego oprogramowania;

5/ zauważeniu elektronicznych śladów próby włamania do systemu informatycznego;

6/ podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe;

7/ zmianie położenia sprzętu komputerowego;

8/ zauważeniu śladów usiłowania włamania lub dokonania włamania do pomieszczeń lub szaf.

2. Do czasy przybycia na miejsce ABI należy:

1/ niezwłocznie w miarę możliwości podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego zdarzenia a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców;

2/ wstrzymać bieżącą pracę na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia;

3/ zaniechać w miarę możliwości dalszych planowanych przedsięwzięć które wiążą się z zaistniałym naruszeniem i mogą utrudniać udokumentowanie i analizę;

4/ zastosować się do instrukcji lub dokumentacji aplikacji odnoszącej się do zaistniałego przypadku;

5/ przygotować opis incydentu;

6/ nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czas przybycia ABI.

3. Pracownik urzędu przyjmujący zawiadomienie jest obowiązany niezwłocznie poinformować ABI o naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu.

4. ABI po otrzymaniu zawiadomienia, o którym mowa w ust. 1 powinien niezwłocznie:

1/ przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych;

2/ podjąć działania chroniące system przed ponownym naruszeniem;

3/ w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego a następnie niezwłocznie przekazać jego kopię administratorowi danych;

5. ABI może zarządzić w razie potrzeby odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.

6. W razie odtwarzania danych z kopii zapasowych administrator obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu.

7. Administrator danych po zapoznaniu się z raportem podejmuje decyzję o dalszym trybie postępowania powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego bądź zastosowaniu środków ochrony fizycznej

8. Administrator bezpieczeństwa informacji zobowiązany jest do informowania administratora o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.

9. Administrator bezpieczeństwa informacji składa raz w roku administratorowi danych analizę zarządzania systemami informatycznymi.

XIV. Postanowienia końcowe.

1. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje i zalecenia producentów wykorzystywanych urządzeń i programów.

2. Każda osoba uprawniona do przetwarzania danych osobowych zobowiązana jest do zapoznania się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie potwierdzające znajomość jej treści.

3. Naruszenie obowiązków wynikających z niniejszej instrukcji oraz przepisów o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych podlegające sankcjom dyscyplinarnym oraz sankcjom karnym wynikającym z ustawy.

Załącznik do instrukcji

Wykaz systemów informatycznych

1. Systemy informatyczne zainstalowane na serwerze w sieci lokalnej, bez połączenia do sieci publicznej:

a/ „Xpertis Kadry i płace”,

b/ „Xpertis Podatek od środków transportowych”,

c/ „Xpertis Podatek rolny, leśny i od nieruchomości”,

d/ „Xpertis Odpady komunalne”,

e/ „Fundusz alimentacyjny”,

f/ „Stypendia szkolne”,

g/ „Świadczenia rodzinne”.

2. Systemy informatyczne zainstalowane na stacjach roboczych nie włączonych do sieci lokalnej, bez połączenia do sieci publicznej:

a/„ SOO - Ewidencja wydanych i utraconych dowodów osobistych ”.

3. Systemy informatyczne zainstalowane na stacjach roboczych włączonych do sieci lokalnej, z połączeniem do sieci publicznej:

a/ „ SELWIN - Ewidencja ludności”,

b/ „Home bankig - System bankowy”,

c/ „PB-USC Rejestracja Stanu cywilnego”,

d/ „APAR - Podatek akcyzowy ”.