ZARZĄDZENIE NR 53
BURMISTRZA MIROSŁAWCA

z dnia 22 maja 2012 r.

w sprawie ustalenia "Polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy i Miasta w Mirosławcu" oraz "Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy i Miasta Mirosławiec".

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U.Nr 101 poz.926 ze zm.) oraz § 3 ust. 3 i § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U.Nr 100, poz. 1024), zarządza się co następuje:

§ 1. Ustala się "Politykę bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy i Miasta w Mirosławcu", stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§ 2. Ustala się "Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy i Miasta Mirosławiec", stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§ 3. Zobowiązuje się pracowników Urzędu Gminy i Miasta w Mirosławcu do stosowania zasad określonych w "Polityce bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy i Miasta w Mirosławcu" oraz w "Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy i Miasta Mirosławiec".

§ 4. Wykonanie Zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik Nr 1 do Zarządzenia Nr .....

Burmistrza Mirosławca

z dnia 22 maja 2012 r.

Polityka bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy i Miasta w Mirosławcu

Dokument „Polityka bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy i Miasta w Mirosławcu", zwana dalej „Polityką bezpieczeństwa" opisuje reguły dotyczące bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy i Miasta Mirosławiec.

Polityka bezpieczeństwa określa ramowe zasady właściwego zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i system informatyczny, odpowiednie do zagrożeń i kategorii danych objętych ochroną.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2002 r. Nr 101, poz. 926, ze zm.) oraz 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) nakłada na administratora danych osobowych następujące obowiązki:

1. zapewnienie bezpieczeństwa i poufności danych, w tym zabezpieczenie ich przed ujawnieniem,
2. zabezpieczenie danych przed nieuprawnionym dostępem,
3. zabezpieczenie danych przed udostępnieniem osobom nieupoważnionym (nieuprawnionym pozyskaniem),
4. zabezpieczenie przed utratą danych,
5. zabezpieczenie przed uszkodzeniem lub zniszczeniem danych oraz przed ich nielegalną modyfikacją.

Ochronie podlegają dane osobowe niezależnie od formy przechowywania, sprzęt komputerowy, systemy operacyjne i informatyczne oraz pomieszczenia, w których odbywa się proces przetwarzania.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami w zakresie prowadzenia właściwej polityki bezpieczeństwa informacji.

Niniejszy dokument wskazuje dopuszczalne zachowanie wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu, procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń oraz sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych.

Rozdział 1.
POSTANOWIENIA OGÓLNE

§ 1. Ilekroć w niniejszym dokumencie jest mowa o:

1. Urzędzie –należy przez to rozumieć Urząd Gminy i Miasta w Mirosławcu.

2. Administratorze Danych Osobowych (ADO) –należy przez to rozumieć Burmistrza Mirosławca.

3. Administratorze Bezpieczeństwa Informacji –należy przez to rozumieć Sekretarza Gminy i Miasta Mirosławiec wyznaczonego do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych.

4. Administratorze Systemu Informatycznego –należy przez to rozumieć firmę zewnętrzną świadczącą usługi informatyczne i administracyjne dla Urzędu lub pracownika Urzędu odpowiadających za funkcjonowanie systemu informatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony.

5. Komórce organizacyjnej- należy przez to rozumieć każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną zgodnie z Regulaminem Organizacyjnym.

6. Użytkowniku systemu -należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym urzędu. Użytkownikiem może być pracownik urzędu, osoba wykonująca pracę na podstawie umowy-zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w urzędzie.

7. Sieci lokalnej –należy przez to rozumieć połączenie systemów informatycznych urzędu wyłącznie dla własnych jego potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.

8. Danych osobowych –należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

9. Zbiorze danych –należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów.

10. Wykazie zbiorów danych osobowych –należy przez to rozumieć wykaz zarejestrowanych oraz nie podlegających rejestracji zbiorów danych osobowych.

11. Przetwarzaniu danych –należy przez to rozumieć jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

12. Systemie informatycznym –należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

13. Bezpieczeństwie systemu informatycznego– należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.

14. Dokumentacji papierowej– należy przez to rozumieć zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierającej dane osobowe.

15. Identyfikatorze użytkownika (LOGIN)– należy przez to rozumieć ciąg znaków literowych i cyfrowych, lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

16. Haśle (Password)– należy przez to rozumieć ciąg znaków literowych cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

§ 2. Cele i strategie bezpieczeństwa informacji.

1. Polityka bezpieczeństwa określa:

1) Zasady postępowania przy przetwarzaniu danych osobowych.

2) Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.

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

4) Sposób przepływu danych pomiędzy poszczególnymi aplikacjami.

5) Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych.

6) Przedsięwzięcia zabezpieczające przed naruszeniem bezpieczeństwa ochrony danych osobowych.

7) Tryb postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych w systemach informatycznych lub dokumentacji papierowej albo powzięcia podejrzenia o takim naruszeniu.

2. Cele i zamierzenia Urzędu Gminy i Miasta w Mirosławcu w dziedzinie bezpieczeństwa informacji:

1) Ochrona zasobów informacyjnych i zapewnienie ciągłości działania procesów Urzędu,

2) Ochrona wizerunku Urzędu,

3) Zapewnienie zgodności z prawem podejmowanych działań,

4) Uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów Urzędu rozumiane jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań,

5) Wyznaczenie ogólnych kierunków rozwoju systemu informacyjnego,

3. Realizację celów i zamierzeń określonych w § 2 ust.1 powinny zagwarantować następujące założenia:

1) Wdrożenie procedur określających postępowania osób zatrudnionych przy przetwarzaniu danych osobowych oraz ich odpowiedzialności za bezpieczeństwo tych danych.

2) Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory), zapewniających im dostęp do różnych poziomów baz danych osobowych – stosownie do indywidualnego zakresu upoważnienia.

3) . Przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych.

4) Podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń.

5) Okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych.

6) Opracowanie procedur odtwarzających w przypadku wystąpienia awarii.

7) Śledzenie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych i w miarę możliwości organizacyjnych i techniczno-finansowych wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

4. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez:

1) Zabezpieczenia fizyczne.

2) Procedury organizacyjne.

3) Oprogramowanie systemowe.

4) Aplikacje.

5) Postępowanie użytkowników.

5. Zastosowane zabezpieczenia gwarantować mają:

1) Poufność danych – należy przez to rozumieć właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

2) Integralność danych – należy przez to rozumieć właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

3) Rozliczalność - należy przez to rozumieć właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

4) Integralność systemu - należy przez to rozumieć nienaruszalność systemu i niemożność dokonania w nim jakiejkolwiek manipulacji.

5) Uwierzytelnienie - należy przez to rozumieć działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Rozdział 2.
PRZETWARZANIE DANYCH OSOBOWYCH

§ 3. Informacje przetwarzane przez system informacyjny Urzędu Gminy

1. W systemie informacyjnym Urzędu przetwarzane są informacje służące do wykonywania zadań z zakresu administracji publicznej.

2. Informacje te są przetwarzane i składowane zarówno w postaci papierowej jak i elektronicznej.

3. Przetwarzane w Urzędzie informacje są między innymi informacjami dotyczącymi

1) informacji publicznych,

2) danych osobowych,

3) informacji stanowiących tajemnice Urzędu,

4) innych informacji prawnie chronionych.

4. Informacje niejawne nie są objęte zakresem niniejszej Polityki.

5. W systemie informatycznym stosuje się wysoki poziom bezpieczeństwa przy przetwarzaniu danych osobowych.

§ 4. 1. **Administrator Danych Osobowych jest zobowiązany do:**

1) czuwania nad tym, by będące w jego posiadaniu dane osobowe były przetwarzane zgodnie z prawem,

2) zastosowania niezbędnych środków technicznych i organizacyjnych w celu zapewnienia ochrony przetwarzanych w Urzędzie danych osobowych,

3) sprawowania kontroli nad bezpieczeństwem oraz sposobem przetwarzania danych,

4) rejestracji w Głównym Inspektoracie Ochrony Danych Osobowych, zbiorów danych przed przystąpieniem do ich przetwarzania, prowadzenia rejestru osób zatrudnionych przy przetwarzaniu danych wg wzoru stanowiącego Załącznik nr 1.1 do niniejszego dokumentu.

2. Administrator Danych Osobowych wyznacza Administratora Bezpieczeństwa Informacji.

3. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:

1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,

2) podejmowania stosownych działań zgodnie z niniejszą Polityką bezpieczeństwa w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,

3) niezwłocznego informowania Administratora Danych Osobowych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,

4) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

4. Czynności przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez Administratora Danych Osobowych lub osoba/firma wykonująca dla Urzędu usługę. Wzór upoważnienia stanowią Załączniki nr 1.2 i 1.3 do niniejszego dokumentu.

5. Pracownik upoważniony przez ADO do przetwarzania danych osobowych, jest zobowiązany do:

1) odbycia wewnętrznego szkolenia dotyczącego przetwarzania i ochrony danych osobowych

2) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,

3) stosowania określonych przez administratora danych, procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,

4) zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których te dane dotyczą,

5) podporządkowania się poleceniom administratora bezpieczeństwa informacji oraz właściwego kierownika, w zakresie ochrony danych.

6. Pracownik, któremu administrator danych osobowych udzielił upoważnienia, o którym mowa w ust. 4 jest zobowiązany do podpisania oświadczenia. Wzór oświadczenia stanowiZałącznik nr 1.4do niniejszego dokumentu.

7. W przypadku zatrudnienia nowego pracownika, zmiany stanowiska, zmiany zakresu obowiązków pracowniczych, utworzenia nowego zbioru danych osobowych, zmiany sposobu przetwarzania danych lub w innych przypadkach, które wpływają bezpośrednio na rodzaj i zakres przetwarzania danych, administrator danych dokonuje cofnięcia lub wydania nowego upoważnienia. Wzór pisma o cofnięciu upoważnienia stanowiZałącznik nr 1.5do niniejszego dokumentu.

8. Wypowiedzenie umowy o pracę jest równoznaczne z cofnięciem upoważnienia do przetwarzania danych osobowych.

9. W obiegu zewnętrznym zgodę na udostępnienie danych osobowych wyraża administrator danych zgodnie z powszechnie obowiązującymi przepisami.

§ 5. Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.

1. Przetwarzanie informacji, w tym informacji osobowych odbywa się w budynku Urzędu Gminy i Miasta w Mirosławcu przy ulicy Wolności 37 w pomieszczeniach zajmowanych przez:

1) Burmistrza Mirosławca (pokój nr 6)

2) Skarbnika Gminy (pokój nr 107)

3) Sekretarza Gminy i Miasta Mirosławiec (pokój nr 7)

4) Referat Organizacyjno-Prawny, (pokój nr 1, 2, 5, 101, 103- serwerownia, 105)

5) Referat Oświaty i Polityki Społecznej, (pokój nr 101, 108)

6) Referat Finansowy, (pokój nr 102, 104)

7) Referat Gospodarki i Środowiska, (pokój nr 8, 9)

8) Urząd Stanu Cywilnego, (pokój nr 4)

9) Samodzielne stanowisko ds. zarządzania kryzysowego, (pokój nr 4)

10) Straż Miejską (pokój nr 3, 3a)

11) Radcę Prawnego (pokój nr 106)

2. Część informacji przetwarzana jest również na komputerach przenośnych.

3. Wszystkie informacje przechowywane są w budynku Urzędu przy ul. Wolności 37.

4. Wszystkie systemy informatyczne Urzędu zlokalizowane są w budynku przy ul. Wolności 37.

§ 6. Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym.

1. Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym prowadzi Administrator Bezpieczeństwa Informacji.

2. Zbiory danych osobowych przetwarzanych w systemie informatycznym wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych wg zestawienia przedstawionego w tabeli.

Lp.	Nazwa zbioru danych	Nazwa programu zastosowanego do ich przetwarzania	Nr pokoju
1.	Urząd Stanu Cywilnego	PB_USC, ZMOKU	4
2	Ewidencja Ludności	SELWIN, ZMOKU	4
3	Dowodowy osobiste	WASKO, ZMOKU	4
4	Rejestr skarg i wniosków	LibreOffice, IBM Lotus Symphony	7
5	Radni Rady Miejskiej	MS Office 2003, IBM Lotus Symphony	105
6	Sołtysi i Rady Sołeckie	MS Office 2003, IBM Lotus Symphony	105
7	Oświadczenia majątkowe	MS Office 2003, LibreOffice, IBM Lotus Symphony	7, 105

8	Postępowanie mandatowe	PIGEON – program finansowo – księgowy, FOTO RAPID, FET TRAFIC P, MS Office 2007, LibreOffice, IBM Lotus Symphony	3, 3a
9	Dofinansowanie doskonalenia zawodowego nauczycieli	MS Office 2007	101
10	Dofinansowanie kształcenia młodocianych pracowników	MS Office 2007	101
11	Stypendia szkolne	MS Office 2007	101
12	Rejestr budowy przydomowych oczyszczalni ścieków	MS Office 2007, LibreOffice, IBM Lotus Symphony	9
13	Sprawy dotyczące usunięcia drzew i krzewów	MS Office 2007, LibreOffice, IBM Lotus Symphony	9
14	Informacje o wyrobach zawierających azbest	MS Office 2007, LibreOffice, IBM Lotus Symphony	9
15	Rejestr decyzji o warunkach zabudowy i zagospodarowania terenu	LibreOffice, IBM Lotus Symphony	8
16	Sprawy dotyczące obronności	MS Office 2003, IBM Lotus Symphony	4
17	Lista osób podlegających kwalifikacji wojskowej	MS Office 2003, IBM Lotus Symphony	4
18	Rejestr mężczyzn lub kobiet objętych rejestracją wojskową	MS Office 2003, IBM Lotus Symphony	4
19	Podatek od środków transportowych	PIGEON – program podatkowy	102
20	Zwrot podatku akcyzowego w cenie oleju napędowego wykorzystywanego do produkcji rolnej	PIGEON – program podatkowy	102
21	Podatki i opłaty lokalne	PIGEON – program podatkowy	102

22	Rejestr dzierżaw mienia komunalnego	LibreOffice, IBM Lotus Symphony	9
23	Rejestr sprzedaży nieruchomości	WebEWID , MS Office 2010, IBM Lotus Symphony	9
24	Ewidencja gruntów	WebEWID, LibreOffice, IBM Lotus Symphony	9
25	Uzależnienia	LibreOffice, IBM Lotus Symphony	108
26	Kadry, Płace	RAKS SQL – program płacowo-kadrowy, PŁATNIK – program do rozliczeń z Zakładem Ubezpieczeń,	101
27	Operacje finansowo-księgowe	GMINA 2 – program finansowo-księgowy,BESTI@ - program finansowo-księgowy, HOME BANKING – system obsługi przelewów bankowych, GMINA z Modułem KASA – system finansowo-księgowy PIGEON, FK ZETO – system finansowo -księgowy w trybie do odczytu, PŁACE – system płacowy w trybie do odczytu, FK PIGEON – program finansowo-księgowy w trybie do odczytu	104 , 107

3. Do przetwarzania danych osobowych w systemie informatycznym urzędu stosuje się ponadto aplikację E-urząd – elektroniczny obieg dokumentów WTF ALFA,

§ 7. Sposób przepływu danych pomiędzy poszczególnymi systemami.

1. Aplikacja RAKS SQL powiązana jest z aplikacją Płatnik w sposób jednokierunkowy poprzez wykonywanie eksportu danych z aplikacji RAKS SQL do aplikacji Płatnik.

2. Aplikacja Gmina 2 powiązana jest z aplikacją BESTI@ w sposób jednokierunkowy poprzez wykonywanie eksportu danych z aplikacji Gmina 2 do aplikacji BESTI@.

3. Pozostałe programy są niezależne i posiadają samodzielne bazy danych.

§ 8. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych wg tabeli.

Lp.	Zbiór danych	Struktura danych
1.	Urząd Stanu Cywilnego	Akt urodzenia: dane dotyczące dziecka (nazwisko, imię (imiona), płeć, data urodzenia, miejsce urodzenia), dane dotyczące rodziców(nazwisko, imię (imiona), nazwisko rodowe, data urodzenia, miejsce urodzenia, miejsce zamieszkania), dane dotyczące osoby (zakładu) zgłaszającego urodzenie(nazwisko i imię (nazwa zakładu), miejsce zamieszkania (siedziba zakładu), przypiski Akt małżeństwa: dane dotyczące osób zawierających małżeństwo(nazwisko, imię(imiona), nazwisko rodowe, stan cywilny, data urodzenia, miejsce urodzenia, miejsce zamieszkania), data i miejsce zawarcia małżeństwa, dane dotyczące rodziców(nazwisko, imię(imiona), nazwisko rodowe), nazwisko noszone po zawarciu małżeństwa, świadkowie(imię i nazwisko), przypiski Akt zgonu: dane dotyczące osoby zmarłej(nazwisko, imię(imiona), nazwisko rodowe, stan cywilny, data urodzenia, miejsce urodzenia, ostatnie miejsce zamieszkania), dane dotyczące daty i miejsca zgonu(data zgonu, godzina zgonu, miejsce zgonu, data znalezienie zwłok, godzina znalezienia zwłok, miejsce znalezienia zwłok), dane dotyczące małżonka osoby zmarłej(nazwisko i imię(imiona), nazwisko rodowe), dane dotyczące rodziców osoby zmarłej (imię, imiona), nazwisko rodowe), dane dotyczące osoby(zakładu) zgłaszającej zgon(nazwisko i imię(nazwa zakładu), miejsce zamieszkania(siedziba zakładu), przypiski
2	Ewidencja	nazwisko i imię, numer ewidencyjny PESEL, adres: kod terytorialny, miejscowość,

	Ludności	ulica, nr domu, nr lokalu, kod pocztowy, rodzaj zameldowania, data zameldowania, data wymeldowania, płeć, nazwisko rodowe, imię ojca, nazwisko ojca, nazwisko rodowe ojca, imię matki, nazwisko matki, nazwisko rodowe matki, dane o urodzeniu: data, miejsce urodzenia, USC: kod terytorialny, nr aktu urodzenia, data wystawienia, stan cywilny, data zmiany, organ: kod terytorialny, nazwa organu, nr aktu, współmałżonek: nazwisko rodowe, imię, nr PESEL, forma ustania małżeństwa, dokument tożsamości, seria i numer, data wystawienia, data ważności, wystawca: kod terytorialny, nazwa wystawcy, rysopis: wzrost w cm, kolor oczu, znak szczególny, obowiązek wojskowy, dokument wojskowy, seria i numer, stopień wojskowy, obywatelstwo obce, data zmiany, podstawa prawna zmiany, grupa krwi, uprawnienia wyborcze, status mieszkańca, rejestr wyborców: nazwisko, imię (imiona), imię ojca, data urodzenia, nr ewidencyjny PESEL, adres zamieszkania: miejscowość, ulica, nr domu, nr mieszkania
3	Dowodowy osobiste	Numer PESEL, siedziba wystawcy, numer dowodu osobistego, organ wystawcy, nazwisko własne 1 człon, nazwisko własne 2 człon, imię własne 1, imię własne 2, nazwisko rodowe 1 człon, nazwisko rodowe 2. człon, imię ojca, imię matki, nazwisko rodowe matki 1. człon, nazwisko rodowe matki 2. człon, data urodzenia, miejsce urodzenia, rodzaj zameldowania, kod pocztowy, kod terytorialny, miejscowość, ulica, numer domu, numer lokalu, poczta zameldowania, kolor oczu, wzrost w cm, płeć, zdjęcie, podpis
4	Rejestr skarg i wniosków	data wpływu, imię i nazwisko petenta, nazwa instytucji, redakcji, adres petenta, instytucji, przedmiot skargi, wniosku, sposób załatwienia, data wysłania zawiadomienia, kogo zawiadomiono
5	Radni Rady Miejskiej	imię i nazwisko, adres, nr PESEL, numer telefonu, adres e-mail, numer konta bankowego
6	Sołtysi i Rady Sołeckie	imię i nazwisko, adres, numer telefonu
7	Oświadczenia majątkowe	miejscowość i dzień wypełnienia oświadczenia, imię i nazwisko, nazwisko rodowe, data i miejsce urodzenia, miejsce zatrudnienia, stanowisko lub funkcja, środki pieniężne zgromadzone w walucie obcej papiery wartościowe, prowadzona działalność gospodarcza (forma prawna i przedmiot działalności), przychód i dochód osiągnięty z prowadzonej działalności gospodarczej, zarządzana działalność gospodarcza (przedstawiciel, pełnomocnik, forma prawna, przedmiot działalności), dochód z zarządzania działalnością gospodarczą, działalność w spółkach handlowych (nazwa i siedziba spółki), czy jest członkiem zarządu(od kiedy), czy jest członkiem rady nadzorczej(od kiedy), czy jest członkiem komisji rewizyjnej(od kiedy), dochody osiągnięte z tego tytułu, działalność w spółdzielniach, czy jest członkiem zarządu(od kiedy), czy jest członkiem rady nadzorczej(od kiedy), czy jest członkiem komisji rewizyjnej(od kiedy), dochody osiągnięte, działalność w fundacjach prowadzących działalność gospodarczą, czy jest członkiem zarządu(od kiedy), czy jest członkiem rady nadzorczej(od kiedy), czy jest członkiem komisji rewizyjnej(od kiedy), dochody osiągnięte, inne dochody z tytułu zatrudnienia lub innej działalności zarobkowej(z podaniem kwot uzyskiwanych z każdego tytułu), dom(powierzchnia, wartość, tytuł prawny), mieszkanie(powierzchnia, wartość, tytuł prawny), gospodarstwo rolne(rodzaj, powierzchnia, wartość, rodzaj zabudowy, tytuł prawny, dochód) , inne nieruchomości(powierzchnia, wartość, tytuł prawny), udziały w spółkach handlowych (liczba, emitent udziałów, dochód), majątek nabyty od skarbu państwa, samorządu w drodze przetargu, składniki mienia ruchomego o wartości powyżej 10.000 zł, zobowiązania pieniężne o wartości powyżej 10.000 zł
8	Postępowani	nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres

	e mandatowe	zamieszkania lub pobytu, numer ewidencyjny PESEL, Numer Identyfikacji Podatkowej, miejsce pracy, zawód, seria i numer dowodu osobistego, numer telefonu
9	Dofinansowanie doskonalenia zawodowego nauczycieli	imię i nazwisko, adres, miejsce pracy, staż pracy, wykształcenie, wysokość dofinansowania
10	Dofinansowanie kształcenia młodocianych pracowników	imię i nazwisko, adres, wykształcenie młodocianego pracownika, uprawnienia pracodawcy do prowadzenia kształcenia zawodowego
11	Stypendia szkolne	imię i nazwisko ucznia, imiona rodziców, adres zamieszkania, PESEL dziecka, informacja o miejscu nauki dziecka, informacja o wysokości dochodów w rodzinie, informacja o funkcjonowaniu rodziny
12	Rejestr budowy przydomowych oczyszczalni ścieków	Imię i nazwisko, adres
13	Sprawy dotyczące usunięcia drzew i krzewów	Imię i nazwisko, nr działki, adres
14	Informacje o wyrobach zawierających azbest	Imię i nazwisko, adres
15	Rejestr decyzji o warunkach zabudowy i zagospodarowania terenu	imię i nazwisko, adres, nr ewidencyjny działki
16	Sprawy dotyczące obronności	imię i nazwisko, adres, numer telefonu
17	Lista osób podlegających kwalifikacji wojskowej	nazwisko, imię (drugie imię), imię ojca, data urodzenia (rok, miesiąc, dzień), seria i numer dowodu osobistego lub innego dokumentu, miejsce aktualnego pobytu (stałego lub czasowego ponad 2 miesiące) – miasto, ulica, numer domu i mieszkania, wezwano na dzień (dzień, miesiąc, rok), zgłosił się dnia, kategoria przydatności do służby wojskowej, nr książeczki wojskowej, uwagi, adnotacje dotyczące przyczyn dopisania lub skreślenia z listy, adnotacje o odwołaniach, sprzeciwach, zmianie

		orzeczenia itp.
18	Rejestr mężczyzn lub kobiet objętych rejestracją wojskową	nazwisko, imię (drugie imię), nazwisko rodowe, imiona i nazwiska rodowe rodziców, data i miejsce urodzenia, stan cywilny, PESEL, adres i data zameldowania na pobyt stały oraz poprzednie adresy, typ wymeldowania, adres zameldowania na pobyt czasowy ponad 3 miesiące
19	Podatek od środków transportowych	imię i nazwisko, adres, imiona rodziców, data urodzenia, PESEL, NIP
20	Zwrot podatku akcyzowego w cenie oleju napędowego wykorzystywanego do produkcji rolnej	imię i nazwisko, adres, PESEL, rodzaj dokumentu stwierdzającego tożsamość, numer, organ wydający dokument, użytki rolne w posiadaniu (we współposiadaniu), użytki rolne razem, ilość zakupionego oleju
21	Podatki i opłaty lokalne	imię i nazwisko, adres, imiona rodziców, data urodzenia, PESEL, NIP
22	Rejestr dzierżaw mienia komunalnego	imię i nazwisko, data zawarcia umowy, data ważności umowy, adres, nr działki, kwota do przypisu, powierzchnia wydzierżawiona, rodzaj użytku, klasa
23	Rejestr sprzedaży nieruchomości	imię i nazwisko lub nazwa, nr działki, powierzchnia, wartość
24	Ewidencja gruntów	imię i nazwisko lub nazwa, nr działki, powierzchnia, wartość
25	Uzależnienia	imię i nazwisko, data urodzenia, imię ojca, imię matki, nazwisko rodowe matki, miejsce zamieszkania, rodzaj uzależnienia
26	Kadry, Płace	PESEL, nazwisko, imię, drugie imię, nazwisko rodowe, nazwisko poprzednie, imię ojca, imię matki, nazwisko rodowe matki, płeć, data urodzenia, miejsce urodzenia, stan cywilny, adres stały: ulica, nr domu, nr lokalu, miejscowość, kod pocztowy, kod, teryt. gminy, gmina, powiat, województwo, adres obecny: ulica, nr domu, nr lokalu, miejscowość, kod pocztowy, kod, teryt. gminy, gmina, powiat, województwo, dokument tożsamości (dowód osobisty): seria i numer, organ wydający, data wydania, konta bankowe, dane dotyczące służby wojskowej: obowiązek wojskowy, służba wojskowa, staż pracy: liczba lat, wykształcenie: szkoła, zawód wyuczony, tytuł zawodowy, telefon,
27	Operacje finansowo-	imię i nazwisko, nazwa, adres, numer konta bankowego

	księgowe	

Rozdział 3.
PRZEDSIĘWZIĘCIA ZABEZPIECZAJĄCE PRZED NARUSZENIEM OCHRONY DANYCH OSOBOWYCH

§ 9. Za naruszenie ochrony danych osobowych uważa się w szczególności:

1. Nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują.

2. Wszelkie modyfikacje danych osobowych lub próby ich dokonywania przez osoby nieuprawnione (np. zmianę zawartości danych, utratę całości lub części danych).

3. Naruszenie lub próby naruszenia integralności systemu.

4. Zmianę lub utratę danych zapisanych na kopiach zapasowych.

5. Naruszenie lub próby naruszenia poufności danych lub ich części.

6. Nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu).

7. Udostępnienie osobom nieupoważnionym danych osobowych lub ich części.

8. Zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji w systemy informatyczne zmierzające do zakłócenia ich działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodnych z przeznaczeniem) danych zawartych w systemach informatycznych lub dokumentacji papierowej.

9. Inny stan systemu informatycznego lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy.

10. Włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

§ 10. Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1. Środki ochrony fizycznej:

1) Budynek Urzędu jest zamykany po zakończeniu pracy.

2) Budynek całodobowo jest dozorowany przez system monitoringu Firmy ANTSERWIS -na zewnątrz budynku oraz wewnątrz zainstalowane są kamery (na zewnątrz jedna kamera od strony głównej budynku oraz druga od strony dziedzińca i wewnątrz budynku na parterze w korytarzu głównym).

3) W budynku Urzędu zainstalowany jest system alarmowy (2 czujniki na parterze – w korytarzu głównym oraz w pokoju nr 9).

4) Od strony dziedzińca budynek jest częściowo okratowany.

5) W budynku Urzędu zgodnie z obowiązującymi przepisami rozmieszczony jest sprzęt przeciwpożarowy.

6) Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osób zatrudnionych i upoważnionych do przetwarzania danych lub w obecności Administratora Bezpieczeństwa Informacji.

7) Pomieszczenia, o których mowa wyżej powinny być zamykane na czas nieobecności pracowników w sposób uniemożliwiający dostęp do nich osób trzecich.

8) W przypadku przebywania interesantów bądź innych osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

9) Do przebywania w pomieszczeniu, gdzie umieszczone są serwery (pokój nr 103) uprawniony jest Administrator Systemu Informatycznego oraz Administrator Bezpieczeństwa Informacji.

10) Przebywanie osób nieuprawnionych w pomieszczeniu, gdzie umieszczone są serwery (np. nieuprawniony pracownik referatu, konserwator, sprzątaczka,) dopuszczane jest tylko w obecności Administratora Sieci Informatycznej lub Administratora Bezpieczeństwa Informacji.

11) Wejście do pomieszczenia z dostępem do systemu CEPIK (pokój 3a) znajduje się wewnątrz pokoju nr 3 położonego na podwyższonym parterze w bocznym korytarzu budynku. Pomieszczenie z dostępem do systemu CEPIK jest pomieszczeniem pozbawionym możliwości innego dostępu do niego lub jego opuszczenia jak przez pokój nr 3 – siedzibę Straży Miejskiej w Mirosławcu. W przypadku wystąpienia zdarzeń mogących skutkować uszkodzeniem komputera mającego dostęp do systemu CEPIK (zalanie, pożar, itp.) pracownik upoważniony do dostępu do bazy danych i przebywania w pomieszczeniu z dostępem do systemu CEPIK ma obowiązek przeniesienia jednostki z systemem CEPIK do pomieszczenia nr 7, gdzie Administrator Bezpieczeństwa Informacji umieści przeniesiony sprzęt w metalowej szafie.

12) Do przebywania w pomieszczeniu z dostępem do systemu CEPIK uprawnione są osoby upoważnione. Inne osoby mogą przebywać w pomieszczeniu jedynie w obecności osób upoważnionych, za ich wiedzą i zgodą.

13) Kopie zapasowe baz danych przechowywane są w metalowej szafie zamykanej na 2 zamki w pokoju nr 7.

2. Środki sprzętowe, informatyczne i telekomunikacyjne

1) Każdy dokument papierowy, zawierający dane osobowe i przeznaczony do zniszczenia, powinien być zniszczony w sposób uniemożliwiający jego odczytanie przy pomocy niszczarki.

2) Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych drzwiami z zamkami patentowymi, z tym że drzwi wewnętrzne prowadzące do pomieszczenia z dostępem do systemu CEPIK są zabezpieczone przed wyważeniem i wyposażone w 1 zamek atestowany (klasa 2 Norma PN-ENV 1627:2006)) a okno pomieszczenia z dostępem do systemu CEPIK oraz okna w pokoju nr 3 zajmowanym przez Straż Miejską zabezpieczone są folią antywłamaniową.

3) Urządzenia wchodzące w skład systemu informatycznego podłączone są do trzech awaryjnych zasilaczy UPS w serwerowni, które zabezpieczają system na wypadek zaniku napięcia albo awarii w sieci zasilającej.

4) Stan instalacji elektrycznej winien zabezpieczać sprzęt informatyczny przed przepięciami, przewężeniami i zwarciami a pośrednio przed wystąpieniem pożaru.

5) Stan techniczny sieci komputerowej winien zabezpieczać system informatyczny przed ingerencją z zewnątrz mogącą spowodować zmianę, kradzież lub utratę bazy danych.

6) Sieć lokalna skonfigurowana jest w topologii gwiazdy.

7) Sieć lokalna podłączona jest do internetu poprzez security router zawierający firewall, IPS, funkcję blokowania adresów internetowych oraz zaawansowany monitor ruchu z funkcją logowania w celu analizy zdarzeń.

8) Sieć lokalna zabezpieczona jest na bieżąco aktualizowanym systemem antywirusowym typu client-serwer, w którym na serwerze zainstalowany jest moduł administrator zarządzający modułami klienckimi na stacjach roboczych.

9) Komputer z dostępem do bazy danych CEPIK jest oznaczony i znajduje się w pomieszczeniu nr 3a.

10) Dostęp do serwera zawierającego dane osobowe zabezpieczony jest hasłem.

11) Kopie zapasowe wykonywane są w cyklach:

a) tygodniowy przyrostowy na streamerze i na dysku zapasowym

b) miesięczny pełny na streamerze i na dysku zapasowym.

3. Środki ochrony w ramach oprogramowania systemu:

1) Dostęp do baz danych osobowych zastrzeżony jest wyłącznie dla uprawnionych pracowników.

2) Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych przechowywanych w systemie informatycznym wyłącznie za pośrednictwem aplikacji wymienionych w § 6.

3) System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu odrębnie dla każdego pracownika.

4) Zastosowano działający w tle program antywirusowy na komputerach użytkowników.

4. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych.

1) Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.

2) Dla każdego użytkownika systemu wyznaczony jest odrębny identyfikator.

3) Użytkownicy mają dostęp do aplikacji umożliwiający dostęp tylko do tych danych osobowych, do których mają uprawnienia.

5. Środki ochrony w ramach systemu użytkowego.

1) Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem.

2) Zastosowano wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika.

3) Zastosowano blokadę hasłem podczas dłuższej nieaktywności użytkownika.

6. Procedury organizacyjne.

1) Dostęp do danych osobowych posiadają osoby, którym udzielono upoważnienia do przetwarzania danych osobowych.

2) Upoważnienia do przetwarzania danych osobowych udziela Administrator Danych Osobowych.

3) Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do pracy zostaną przeszkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz poinformowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym.

4) Administrator Bezpieczeństwa Informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz osób upoważnionych do dostępu do bazy danych i pomieszczenia z dostępem do CEPIK .

5) Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na sprzęt nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

6) Za organizację szkoleń odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

7) Wprowadzono instrukcję zarządzania systemem informatycznym.

8) Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.

9) Wprowadzono obowiązek rejestracji wszystkich przypadków awarii systemu, działań konserwacyjnych w systemie oraz naprawy systemu.

10) Określono sposób postępowania z nośnikami informacji.

11) W przypadku, gdy zachodzi konieczność naprawy sprzętu poza siedzibą urzędu, należy wymontować z niego nośniki informacji zawierające dane osobowe.

7. Postępowanie użytkowników.

1) Użytkownicy powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych.

2) Użytkownicy powinni przestrzegać zasad i procedur ochrony danych osobowych w czasie pracy a także po jej zakończeniu.

3) Użytkownicy powinni przestrzegać zasad związanych z otwieraniem i zamykaniem pomieszczeń, a także z wchodzeniem do obszarów przetwarzania danych osobowych osób nieupoważnionych.

4) Użytkownicy powinni zwracać szczególną uwagę na sytuacje nietypowe i ewentualne zagrożenia oraz informować o nich Administratora Bezpieczeństwa Informacji.

5) Użytkownicy odpowiedzialni są za rzetelne prowadzenie dokumentacji papierowej, ich kompletność oraz ochronę.

6) Dokumentację papierową oraz nośniki informacji należy przechowywać w przeznaczonych do tego celu szafach biurowych zamykanych na klucz, do których dostęp mają wyłącznie użytkownicy.

7) Klucze do pomieszczeń przechowywane są w wyznaczonym pomieszczeniu, tj. w sekretariacie Burmistrza pokój nr 5.

8) Klucze wydawane są osobom do tego uprawnionym.

9) Klucze zapasowe do pomieszczeń przechowywane są w pokoju nr 7 i mogą być wydawane w sytuacjach awaryjnych, klucz zapasowy do pokoju nr 7 jest dołączony do kompletu kluczy do drzwi wejściowych budynku będących w dyspozycji Burmistrza.

10) Klucze główne oraz zapasowe do szaf przechowywane są przez użytkowników.

11) Klucze do budynku są w dyspozycji osób uprawnionych.

Rozdział 4.

NARUSZENIE OCHRONY DANYCH OSOBOWYCH.

§ 11. Procedura postępowania w przypadku naruszenia ochrony danych osobowych.

1. Każdy pracownik Urzędu, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to Administratorowi Bezpieczeństwa Informacji.

2. W razie braku możliwości zawiadomienia Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej, należy zawiadomić bezpośredniego przełożonego.

3. Do czasu przybycia na miejsce Administratora Bezpieczeństwa Informacji należy:

1) niezwłocznie podjąć czynności niezbędne do powstrzymania skutków naruszenie ochrony (o ile to możliwe),

2) ustalić przyczynę i sprawcę naruszenia ochrony,

3) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia, o ile to możliwe należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia ochrony i udokumentowanie zdarzenia,

4) podjąć stosowne działania, jeśli zaistniały przypadek został przewidziany w dokumentacji systemu operacyjnego, bazy danych, czy instrukcji aplikacji użytkowej,

5) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji.

4. Po przybyciu na miejsce naruszenia bezpieczeństwa danych osobowych Administrator Bezpieczeństwa Informacji podejmuje następujące kroki:

1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy urzędu,

2) może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,

3) powiadamiania o zaistniałym naruszeniu Administratora Danych Osobowych,

4) nawiązuje kontakt ze specjalistami spoza Urzędu (jeśli zachodzi taka potrzeba).

5. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącegoZałącznik nr 1.6do Polityki Bezpieczeństwa.

6. Raport z wystąpienia zdarzenia Administrator Bezpieczeństwa Informacji przekazuje Administratorowi Danych Osobowych.

7. Administrator Bezpieczeństwa Informacji zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń, oraz terminu wznowienia przetwarzania danych osobowych).

8. Zaistniałe naruszenie bezpieczeństwa może stać się przedmiotem zespołowej analizy przeprowadzanej przez Administratora Danych Osobowych, Administratora Bezpieczeństwa Informacji oraz Administratora Sieci Informatycznych.

9. Analiza ta powinna zawierać ocenę zaistniałego naruszenia bezpieczeństwa, wskazanie odpowiedzialnych, wnioski co do ewentualnych działań proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

10. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.

§ 12. Znajomość Polityki Bezpieczeństwa.

Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy Urzędu upoważnieni do przetwarzania danych w systemie informatycznym. Wzór wykazu osób, które zapoznały się z „Polityką bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy i Miasta w Mirosławcu" oraz „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy i Miasta w Mirosławcu" stanowiZałącznik Nr 1.7do Polityki bezpieczeństwa.

§ 13. Postanowienia końcowe.

W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002r. Nr 101, poz. 926), rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).

Załącznik Nr 1.1 do Zarządzenia Nr .....
Burmistrza Mirosławca
z dnia 22 maja 2012 r.

Rejestr osób uprawnionych do przetwarzania danych osobowych

L.p.	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia Przyczyna ustania	Zakres upoważnienia	Podpis ABI
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					

20					
21					

Załącznik Nr 1.2 do Zarządzenia Nr .....

Burmistrza Mirosławca

z dnia 22 maja 2012 r.

Upoważnienie (wzór 1)

……. Mirosławiec, dnia …… r.

(pieczątka)

UPOWAŻNIENIE NR ……..

do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) upoważniam Panią / Pana:

....

(imię i nazwisko osoby upoważnionej)

zatrudnioną (ego) w:

....

(nazwa jednostki i komórki organizacyjnej)

na stanowisku: .....

do przetwarzania od dnia .....20…..… r. danych osobowych

w zakresie ....

oraz do obsługi systemu informatycznego i urządzeń wchodzących w jego skład służących do przetwarzania danych osobowych.

Upoważnienie wydaje się na czas zatrudnienia w Urzędzie Gminy i Miasta w Mirosławcu.

.....

(podpis administratora danych)

……..….

(data i podpis pracownika)

Załącznik Nr 1.3 do Zarządzenia Nr .....

Burmistrza Mirosławca

z dnia 22 maja 2012 r.

Upoważnienie (wzór 2)

……. Mirosławiec, dnia ……

r.

(pieczątka)

UPOWAŻNIENIE NR ……..
do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) upoważniam Panią / Pana:

.....

(imię i nazwisko osoby upoważnionej/nazwa firmy)

wykonującą/wykonującego dla Urzędu Gminy i Miasta w Mirosławcuusługę w zakresie

na podstawie umowy ….....

do przetwarzania od dnia .....20…..… r. danych osobowych

w zakresie ....

oraz do obsługi systemu informatycznego i urządzeń wchodzących w jego skład służących do przetwarzania danych osobowych.

Upoważnienie wydaje się na czas umowy zawartej na wykonanie usługi.

.....

(podpis administratora danych)

……..….....

(data i podpis osoby upoważnionej)

Załącznik Nr 1.4 do Zarządzenia Nr .....
Burmistrza Mirosławca
z dnia 22 maja 2012 r.

Oświadczenie (wzór)

……....
(imię i nazwisko pracownika)
….....
(stanowisko)

OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana jest mi treść przepisów:

a) o ochronie tajemnic prawnie chronionych stanowiących tajemnicę służbową wynikającą z Kodeksu Pracy,

b) o ochronie danych osobowych wynikających z ustawy o ochronie danych osobowych,

c) o odpowiedzialności karnej za naruszenie ochrony danych osobowych.

2. Zobowiązuje się nie ujawniać wiadomości, z którymi zapoznałem/am się w trakcie wykonywania czynności służbowych.

Mirosławiec, dnia ……

……

(podpis pracownika)

Załącznik Nr 1.5 do Zarządzenia Nr .....

Burmistrza Mirosławca

z dnia 22 maja 2012 r.

WYCOFANIE UPOWAŻNIENIA (wzór)

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.)

w związku z:
……
……
……
……

cofam upoważnienie

Pana/Pani

…….....
.....

zatrudnionego/zatrudnionej w ……..
.....

na stanowisku
……..... .....

do przetwarzania danych osobowych w zakresie.....

…….

(data i podpis Administratora Danych Osobowych)

Otrzymałem(łam) dnia:

Mirosławiec, dnia ….....r. ……

(podpis pracownika)

Załącznik Nr 1.6 do Zarządzenia Nr .....

Burmistrza Mirosławca

z dnia 22 maja 2012 r.

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W URZĘDZIE GMINY I MIASTA W MIROSŁAWCU (wzór)

1. Data: ..... Godzina: .....

   (dd.mm.rrrr) (gg:mm)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

   ....

   (imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)

3. Lokalizacja zdarzenia:

   ....

   (np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

   .....

   .....

   .....

5. Przyczyny wystąpienia zdarzenia:

   .....

   .....

   .....

6. Podjęte działania:

   .....

   .....

   .....

7. Postępowanie wyjaśniające:

   .....

   .....

   .....

   ……..

   (data, podpis Administratora Bezpieczeństwa Informacji)

Załącznik Nr 1.7 do Zarządzenia Nr .....

Burmistrza Mirosławca

z dnia 22 maja 2012 r.

Wykaz osób, które zapoznały się z „Polityką bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy i Miasta w Mirosławcu" oraz „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy i Miasta w Mirosławcu" (wzór)

Lp.	Imię i Nazwisko	Stanowisko	Data	Podpis

Załącznik Nr 2 do Zarządzenia Nr .....

Burmistrza Mirosławca

z dnia 22 maja 2012 r.

Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Urzędzie Gminy i Miasta w Mirosławcu

Celem Instrukcji Zarządzania System Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy i Miasta w Mirosławcu, zwanej dalej „Instrukcją" jest zapewnienie bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy i Miasta w Mirosławcu , oraz minimalizowanie incydentów mogących zagrozić bezpieczeństwu systemu.

§ 1. Ilekroć w niniejszym dokumencie jest mowa o:

1. Urzędzie - należy przez to rozumieć Urząd Gminy i Miasta w Mirosławcu,

2. Administratorze Danych Osobowych (ADO) - należy przez to rozumieć Burmistrza Mirosławca.

3. Administratorze Bezpieczeństwa Informacji (ABI) - należy przez to rozumieć Sekretarza Gminy i Miasta Mirosławiec wyznaczonego do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych.

4. Administratorze Systemu Informatycznego (ASI)- należy przez to rozumieć firmę zewnętrzną świadczącą usługi informatyczne i administracyjne dla Urzędu lub pracownika Urzędu odpowiadających za funkcjonowanie systemu informatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony.

5. Użytkowniku systemu - należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym urzędu. Użytkownikiemmoże być pracownik urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w urzędzie.

6. Sieci lokalnej - należy przez to rozumieć połączenie systemów informatycznych urzędu wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.

7. Sieci rozległej - należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia16 lipca 2004 r. - Prawo telekomunikacyjne (Dz.U.Nr 171, poz.1800, ze zm.).

8. Danych osobowych – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

9. Zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów.

10. Wykazie zbiorów danych osobowych – rozumie się przez to wykaz zarejestrowanych oraz nie podlegających rejestracji zbiorów danych osobowych.

11. Przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach Informatycznych.

12. Systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

13. Identyfikatorze użytkownika (LOGIN) – należy przez to rozumieć ciąg znaków literowych i cyfrowych, lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

14. Haśle (Password) – należy przez to rozumieć ciąg znaków literowych cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

15. Zalogowaniu – należy przez to rozumieć uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

16. Komórce organizacyjnej - należy przez to rozumieć każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną zgodnie z Regulaminem Organizacyjnym.

17. Polityce Bezpieczeństwa - należy przez to rozumieć Politykę Bezpieczeństwa Danych Osobowych Przetwarzanych w Urzędzie Gminy i Miasta w Mirosławcu.

§ 2. Procedury nadawania i zmiany uprawnień do przetwarzania danych.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych jest zobowiązany do zapoznania się z:

1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 ze zm.),

2) polityką bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy i Miasta w Mirosławcu,

3) niniejszym dokumentem.

2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi Załącznik nr 1 do Polityki Bezpieczeństwa .

3. Przetwarzania danych osobowych może dokonywać jedynie osoba upoważniona przez

administratora danych osobowych.

4. Administrator Danych Osobowych upoważnia pracownika lub osobę/firmę wykonującą dla Urzędu usługę, do przetwarzania danych osobowych oraz przyznaje mu uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia określającego zakres uprawnień, którego wzór stanowią Załączniki nr 2 i 3 do Polityki Bezpieczeństwa.

5. Każdemu użytkownikowi komputera zakłada się oddzielne konto, konta te nie mogą mieć uprawnień administratora, o ile nie jest to wymagane przy bieżącej pracy.

6. Przyznanie dostępu do systemu informatycznego polega na wprowadzeniu przez Administratora Systemu Informatycznegodo systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz nadanie mu uprawnień.

7. Ustanowione identyfikator i hasło, Administrator Systemu Informatycznego przekazuje użytkownikowi ustnie. Hasło to należy zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym.

8. Hasła gromadzone są w usłudze kontroli dostepu w sposób niejawny, gdzie zapisywany jest tylko skrót (password hash), treść hasła znana jest tylko osobie je ustanwiającej.

9. Użytkownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.

10. Użytkownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego

identyfikatora i hasła dostępu.

11. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.

12. Użytkownik zobowiązany jest do zachowania przetwarzanych danych w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.

13. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.

14. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być

tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.

15. Odebranie uprawnień pracownikowi następuje na pisemny wniosek Administratora Bezpieczeństwa Informacji przez Administratora Danych osobowych z podaniem daty oraz przyczyny odebrania uprawnień wg Załącznika Nr 4 do Polityki Bezpieczeństwa.

16. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora

Bezpieczeństwa Informacji o każdej zmianie dotyczącej podległych pracowników mającej

wpływ na zakres posiadanych uprawnień w systemie informatycznym.

17. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.

18. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia rejestru osób uprawnionych do przetwarzania danych osobowych wg wzoru stanowiącego Załącznik nr 5 do Polityki Bezpieczństwa.

19. Rejestr powinien odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników.

§ 3. Zasady ustalania i posługiwania się hasłami.

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Hasło użytkownika powinno być zmieniane co najmniej raz w miesiącu.
3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
7. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, należy natychmiast dokonać zmiany hasła.
8. Przy wyborze hasła obowiązują następujące zasady:

1) minimalna długość hasła - 6 znaków, przy czym długosc hasła administratora lub użytkownika z uprawnieniami administratora nie mniej niż 8 znaków,
2) zakazuje się stosować:
   a) haseł, które użytkownik stosował uprzednio w okresie minionego roku,
   b) swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),
   c) ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, itp.
   d) odpornych na "atak słownikowy",
   e) przewidywalnych sekwencji znaków z klawiatury np.: "QWERTY", "12345678",itp.
3) należy stosować:
   a) hasła zawierające kombinacje liter i cyfr,
   b) hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole: @, #, &, itp. o ile system informatyczny na to pozwala,
   c) hasła, które można zapamiętać bez zapisywania,
   d) hasła łatwe i szybkie do wprowadzenia, po to by trudniej było zidentyfikować je osobom trzecim,

9. Zmiany hasła nie wolno zlecać innym osobom.
10. W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.

11. Hasło administratora lub użytkownika z uprawnieniami administratora powinno znajdować się w zamkniętej kopercie w zamykanej na klucz szafie metalowej, do której dostęp mają:

1) Administrator Bezpieczeństwa Informacji,

2) Burmistrz lub Zastępca Burmistrza.

§ 4. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

1. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu

przy użyciu indywidualnego identyfikatora oraz hasła.

2. Zastosowano wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika.

3. Zastosowano blokadę hasłem podczas dłuższej nieaktywności użytkownika.

4. Przy opuszczeniu stanowiska pracy na dłuższy czas należy wykonać opcję wylogowania z systemu (zablokowania dostępu), lub jeżeli taka możliwość nie istnieje wyjść z programu.

5. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi

zobowiązana jest wykonać funkcję wylogowania z systemu.

6. Czynnością niezbędą do prawidłowego zakończenia pracy jest zamknięcie lub wylogowanie się z systemu.

7. Przypadki stwierdzenia nieprawidłowości systemu należy zgłaszać do Administratora Systemu Informatycznego.

§ 5. Procedury tworzenia kopii bezpieczeństwa.

1. Za systematyczne wykonywanie kopii bezpieczeństwa (kopie zapasowe baz danych) odpowiada Administrator Systemu Informatycznego.

2. Kopie bezpieczeństwa wykonywane są w cyklach:

a) tygodniowy przyrostowy na streamerze i na dysku zapasowym,

b) miesięczny pełny na streamerze i na dysku zapasowym.

3. Kopie bezpieczeństwa przechowywane są w metalowej szafie zamykanej na 2 zamki w pokoju nr 7.

4. Dostęp do w/w mają:

1) Administrator Bezpieczeństwa Informacji

2) Burmistrz.

5. Raz w roku następuje klasyfikacja nośników z kopiami bezpieczeństwa co do dalszej przydatności.

6. Kopie bezpieczeństwa sklasyfikowane jako nie przydatne niszczone są w specjalnej niszczarce.

7. Kopie oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w serwerowni.

§ 6. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji.

zawierających dane osobowe oraz wydruków z zastrzeżeniem § 5 dotyczącego sposobu postępowania z kopiami bezpieczeństwa.

1. Elektroniczne nośniki informacji

1) Dane osobowe w postaci elektronicznej zapisane na płytach CD, DVD, pamięci USB czy dyskach twardych, nie są wynoszone poza siedzibę urzędu.

2) Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w „Polityce Bezpieczeństwa Danych Osobowych przetwarzanych w Urzędzie Gminy i Miasta w Mirosławcu".

3) Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane wyłącznie w zamykanych szafach biurowych.

4) Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, poddaje się bezpiecznemu usuwaniu danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie poddaje się bezpiecznemu usuwaniu danych.

5) Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych .

6) Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, poddaje się bezpiecznemu usuwaniu danych, albo naprawia się je pod nadzorem osoby upoważnionej.

7) Zabrania się używać elektronicznych nośników informacji pochodzących z zewnątrz Urzędu.

2. Wydruki

1) W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym dostęp osobom nieuprawnionym.

2) Pomieszczenie, w którym przechowywane są wydruki musi być zamknięte na klucz po godzinach pracy Urzędu.

3) Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie (w specjalnej niszczarce do papieru).

§ 7. Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi.

1. Za ochronę antywirusową odpowiada Administrator Systemu Informatycznego.

2. Czynności związane z ochroną antywirusową systemu informatycznego wykonuje Administrator Systemu Informatycznego, wykorzystując w trakcie pracy systemu informatycznego moduły programu antywirusowego w aktualnej wersji, sprawdzającego na bieżąco zasoby systemu informatycznego.

3. Oprogramowanie antywirusowe jest instalowane na wszystkich stanowiskach komputerowych podłączonych do sieci.

4. Aktualizacja oprogramowania antywirusowego odbywa się na bieżąco w sposób automatyczny dla wszystkich komputerów.

5. Użytkownik systemu na stanowisku komputerowym, importujący dane do systemu informatycznego, jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów i szkodliwego oprogramowania.

6. W razie stwierdzenia naruszenia ochrony danych osobowych należy postępować zgodnie z procedurą określoną w Polityce Bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy i Miasta w Mirosławcu.

§ 8. Połączenie do sieci Internet.

1. Połączenie lokalnej sieci komputerowej urzędu z Internetem jest dopuszczalne wyłącznie po zainstalowaniu mechanizmów ochronnych oraz kompleksowego oprogramowania antywirusowego.

2. Do zabezpieczenia dostępu do sieci WAN zastosowano zabezpieczenia brzegowe typu security router zawierający firewall (filtruje dane przechodzące pomiędzy siecią lokalną i siecią publiczną, umożliwia stosowanie zasad i polityk w ruchu), IPS (system wykrywania oraz zapobiegania zdalnej penetracji) oraz funkcję blokowania adresów internetowych, wbudowany skaner antywirusowy (z innym silnikiem niż stosowany na poziomie serwera/komputerów) oraz zaawansowany monitor ruchu z funkcją logowania w celu analizy zdarzeń.

§ 9. Środki ochrony w ramach oprogramowania systemu.

1. Dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla osoby zajmującej się obsługą informatyczną urzędu i Administratora Bezpieczeństwa Informacji.

2. Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji.

3. System informatyczny z jakiego korzystają pracownicy Urzędu pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.

4. Wszelkie zmiany dotyczące oprogramowania systemu – instalacje, aktualizacje, usuwanie programów lub inna ingerencja w zasoby informatyczne Urzędu zastrzeżone są do obowiązków Administratora Systemu Informatycznego. Inna osoba musi w tym celu posiadać zgodę lub upoważnienie od Administratora Danych Osobowych lub Administratora Bezpieczeństwa Informacji.

§ 10. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych. 1. Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.

2. Dla każdego użytkownika systemu jest ustalony odrębny identyfikator.

3. Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło).

§ 11. Środki ochrony w ramach systemu użytkowego.

1. Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.

2. Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem logowania do domeny oraz hasłem do każdej aplikacji, przy pomocy której przetwarzane są dane osobowe.

3. W przypadku użycia komputera przenośnego do pracy służbowej poza budynkiem Urzędu należy zachować szczególną ostrożność przez osobę użytkującą podczas transportu, przechowywania oraz użytkowania komputera w celu zapobieżenia dostępu do danych w nim zawartych osobom nieuprawnionym, w szczególności poprzez zabezpieczenie dostępu do komputera hasłem i nie zezwalanie na używanie komputera osobom nieuprawnionym oraz przechowywanie danych na dysku szyfrowanym .

4. Sieć komputerowa oraz stanowiska pracy nie mogą być wykorzystywane w celach innych niż służbowe.

5. Dostęp do lokalnej sieci komputerowej ograniczony jest do urządzeń zautoryzowanych przez urządzenia kontroli dostępu.

6. Zabrania się użytkownikom systemu informatycznego otwierania podejrzanych wiadomości oraz załączników tych wiadomości.

7. Sieć komputerowa monitorowana jest przez Administratora Sieci Informatycznej.