URZĄD GMINY MASŁÓW
ul. Spokojna 2, 26-001 Masłów
REG.000547313, NIP 657 17 48 114

Zarządzenie Nr 183/2015

Wójta Gminy Masłów z dnia 05.11.2015 roku

w sprawie dokumentacji przetwarzania danych w Urzędzie Gminy Masłów

Na podstawie art.33, ust 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tj. Dz.U. z 2013r, poz 594 z pózn. zmianami), w związku z art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 poz. 1182 z pózn. zm.) oraz §3, §4, §5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100, poz.1024) zarządzam, co następuje:

§ 1 .

Wprowadzam dokumentacje określające sposób przetwarzania danych osobowych w Urzędzie Gminy Masłów oraz stosowane środki techniczne i organizacyjne zapewniające ich ochronę w skład której wchodzą:

1) „Polityka bezpieczeństwa przetwarzania danych osobowych", w brzmieniu stanowiącym załącznik nr 1 do zarządzenia;

2) „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych", w brzmieniu stanowiącym załącznik nr 2 do zarządzenia:

§ 2 .

Zobowiązuję wszystkich pracowników Urzędu Gminy Masłów do stosowania i przestrzegania zasad ujętych w dokumentach o których mowa w § 1

§ 3 .

Odpowiedzialnym za wdrożenie, nadzorowanie i przestrzeganie zasad określonych w instrukcjach wymienionych w § 1 czynię Administratora Bezpieczeństwa Informacji - upoważnionego informatyka Urzędu Gminy.

§ 4 .

Traci moc zarządzenie Nr 134/2012 Wójta Gminy Masłów z dnia 28 sierpnia 2012 roku w sprawie zatwierdzenia instrukcji regulującej sprawy ochrony danych osobowych w Urzędzie Gminy w Masłowie.

§ 6 .

Upoważnienia do przetwarzania danych osobowych nadane przez Wójta Gminy Masłów na podstawie dotychczas obowiązujących przepisów, zachowują swą moc do czasu nadania nowych upoważnień.

§ 7 .

Nadzór nad wykonaniem zarządzenia powierza się Sekretarzowi Gminy.

§ 7.

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr Tomasz Lato

URZĄD GMINY MASŁÓW
ul. Spokojna 2, 26-001 Masłów
REG.000547313, NIP 657 17 48 114

Załącznik nr. 1 do Zarządzania NR 183/2015
Wójta Gminy Masłów
Z dnia 05.11. 2015 roku

Polityka Bezpieczeństwa

Polityka Bezpieczeństwa Przetwarzania Danych Osobowych Urzędu Gminy Masłów

Urząd Gminy
Masłów

26-001 Masłów
Ul. Spokojna 2
Powiat Kielecki
Województwo
Świętokrzyskie

www.maslow.pl
gmina@maslow.pl

Wstęp

Celem polityki bezpieczeństwa przetwarzania danych w tym danych osobowych jest zabezpieczenie przetwarzania informacji stanowiących dane osobowe w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182, z późn. zm.). oraz realizacja § 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. z 2004 r. Nr 100, poz. 1024)

Spis treści

1. Definicje

Ilekroć w niniejszej Polityce Bezpieczeństwa Przetwarzania Danych Osobowych mowa o:

1) **komórce organizacyjnej** – rozumie się przez to odpowiednio wydziały i komórki organizacyjne, o których mowa w Rozdziale III §8 - §16 Regulaminu Organizacyjnego Urzędu Gminy w Masłowie stanowiącego załącznik do Zarządzenia Nr 201/2013 Wójta Gminy Masłów z dnia 31 grudnia 2013 roku.

2) **Kierowniku komórki organizacyjnej** – rozumie się przez to kierownika wydziału, referatu, biura, koordynatora i samodzielne stanowiska pracy;

3) **Administratorze Danych Osobowych** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych. Administratorem Danych Osobowych jest Wójt Gminy Masłów;

4) **Administratorze Bezpieczeństwa Informacji** – rozumie się przez to pracownika Urzędu Gminy wyznaczonego przez Administratora Danych Osobowych, nadzorującego przestrzeganie zasad, o których mowa w art. 36 ust. 1 u.o.d.o.;

5) **Administratorze Systemów Informatycznych** – rozumie się przez to pracownika Urzędu Gminy, odpowiedzialnego za funkcjonowanie systemów i sieci teleinformatycznych oraz za przestrzeganie zasad i wymogów bezpieczeństwa systemów i sieci teleinformatycznych;

6) **Osobie upoważnionej** – rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych. Użytkownikiem może być pracownik Urzędu Gminy, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, a także osoba odbywająca wolontariat, praktykę lub staż.

7) **Osobie nieupoważnionej** – rozumie się przez to osobę nieposiadającą upoważnienia do przetwarzania danych osobowych;

8) **Osobie nieuprawnionej** – rozumie się przez to osobę nieposiadającą uprawnień nadanych w systemie informatycznym Urzędu Gminy;

9) **Danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na

numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość;

10) **Zbiorze danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

11) **Przetwarzaniu danych osobowych** – 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) **Zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

14) **Bezpieczeństwie informacji** – rozumie się przez to zespół zasad, jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania informacji by w każdych okolicznościach dostęp do nich był zgodny z założeniami;

15) **Usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

16) **Zgodzie osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgoda może być odwołana w każdym czasie;

17) **Odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe za wyjątkiem:

    a) osoby, której dane dotyczą,

    b) osoby upoważnionej do przetwarzania danych osobowych,

    c) przedstawiciela, o którym mowa w art. 31a u.o.d.o.,

d) podmiotu, o którym mowa w art. 31 u.o.d.o.,

e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

18) **Państwie trzecim** – rozumie się przez to państwo należące do Europejskiego Obszaru Gospodarczego;

19) **Haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi uprawnionemu do pracy w systemie informatycznym;

20) **Identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w wyznaczonych przez Administratora Danych Osobowych obszarach systemu informatycznego Urzędu Gminy;

21) **Teletransmisji danych** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnych;

22) **Poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;

23) **Integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

24) **Rozliczalności danych** – rozumie się przez to właściwość zapewniającą, że działania osoby lub podmiotu mogą być przypisane w sposób jednoznaczny tylko tej osobie lub podmiotowi;

25) **Użytkowniku systemu informatycznego** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych w systemach informatycznych, której nadano unikalny identyfikator i hasło

26) **Uwierzytelnieniu** – rozumie się przez to proces poprawnej identyfikacji użytkownika systemu informatycznego w stopniu umożliwiającym przyznanie odpowiednich uprawnień lub przywilejów w systemie informatycznym Urzędu Gminy;

27) **Sieci komputerowej** – rozumie się przez to grupę komputerów lub innych urządzeń połączonych ze sobą w celu wymiany danych lub współdzielenia różnych zasobów;

28) **Sieci lokalnej** – rozumie się przez to sieć przeznaczoną do łączenia ze sobą stanowisk komputerowych znajdujących się w Urzędzie Gminy;

29) **Sieć publicznej** – rozumie się przez to sieć publiczną w rozumieniu art. 2 ust. 22 ustawy z dnia 21 lipca 2000 r. Prawo telekomunikacyjne (Dz. U. nr 73, poz. 852 z późn. zm.);

30) **Punkcie dystrybucyjnym** – rozumie się przez to miejsce, w którym zlokalizowana jest infrastruktura teleinformatyczna oraz urządzenia umożliwiające dystrybucję połączeń sieciowych w systemie informatycznym Urzędu Gminy;

31) **Stacji roboczej** – rozumie się przez to komputer użytkownika systemu informatycznego podłączony do sieci lokalnej Urzędu Gminy;

32) **Incydent** – rozumie się przez to naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność;

33) **Zagrożenie** - rozumie się przez to potencjalną możliwość wystąpienia incydentu;

34) **Działa korygujące** – rozumie się przez to działanie przeprowadzone w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji;

35) **Działania zapobiegawcze** – rozumie się przez to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej.

2. Zakres stosowania Polityki Bezpieczeństwa Przetwarzania Danych Osobowych

Zakresy określone przez Politykę Bezpieczeństwa Danych Osobowych mają zastosowanie do całego systemu informacyjnego Urzędu Gminy Masłów, a w szczególności do:

1) wszelkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz zbiorów prowadzonych w formie tradycyjnej, w których przetwarzane są dane osobowe;

2) informacji zawierających dane osobowe, których Administratorem Danych Osobowych jest Wójt Gminy Masłów lub przetwarzanych w celu realizacji zadań zleconych Gminie, a których administratorem są organy centralne administracji rządowej lub samorządowej;

3) wszystkich nośników magnetycznych, optycznych lub papierowych, na których są lub będą znajdować się informacje zawierające dane osobowe;

4) wszystkich obszarów (budynki, pomieszczenia, części pomieszczeń), w których są lub będą przetwarzane dane osobowe;

5) wszystkich pracowników Urzędu Gminy w rozumieniu przepisów Kodeksu Pracy, stażystów, praktykantów, wolontariuszy a także innych podmiotów lub osób fizycznych, które współuczestniczą w procesie przetwarzania danych osobowych.

3. Podstawa prawna

Polityka Bezpieczeństwa Danych Osobowych odnosi się do sposobu przetwarzania danych osobowych oraz środków ich ochrony określonych w:

1) ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r. poz. 1182, ze zm.)

2) rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r., Nr 100, poz. 1024);

3) rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r., Nr 229 poz. 1536);

4) ustawie z dnia 18 września 2001 r. o podpisie elektronicznym (t.j. Dz. U. 2013 poz. 262);

5) ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. 2013 poz. 1422);

6) rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. 2007 nr 10 poz. 68);

7) rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2012 poz. 526 ze zm.)

8) rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz. U. z 2006 r., Nr 206, poz. 1517);

9) rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz. U. z 2006 r., Nr 206, poz. 1518);

10) rozporządzeniu Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz. U. z 2002 r., Nr 167, poz. 1375).

4. Struktura dokumentów Polityki Bezpieczeństwa Przetwarzania Danych Osobowych

Zestaw dokumentacji Polityki Bezpieczeństwa Przetwarzania Danych Osobowych składa się z:

1) Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Masłów.

2) Wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;

3) Wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

4) Opisu struktury zbiorów danych osobowych;

5) Opisu sposobu przepływu danych pomiędzy poszczególnymi systemami;

6) Określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych;

7) Wzorów formularzy pomocniczych.

Wyżej wymienione dokumenty będą prowadzone w formie odrębnej dokumentacji, przez Administratora Bezpieczeństwa Informacji na podstawie wzorów stanowiących załączniki do niniejszej Polityki Bezpieczeństwa Przetwarzania Danych Osobowych.

5. Zakres rozpowszechniania

Z treścią niniejszej Polityki Bezpieczeństwa Danych Osobowych powinny zapoznać się wszystkie osoby posiadające dostęp do danych osobowych na podstawie nadanych upoważnień przez Administratora Danych Osobowych.

Dokument ten może być także udostępniany partnerom przetwarzającym dane osobowe Urzędu, z którym Urząd Gminy Masłów związany jest odpowiednimi umowami.

6. Obowiązki Administratora Danych Osobowych

Do podstawowych obowiązków Administratora Danych Osobowych należy:

1) przetwarzanie danych osobowych zgodnie z prawem;

2) dopełnienie obowiązku zgłoszenia zbiorów danych osobowych do rejestracji GIODO, za wyjątkiem przypadków określonych w art. 43 ustawy. Obowiązkowi rejestracji zbiorów danych osobowych z wyjątkiem zbiorów zawierających dane wrażliwe nie podlega administrator danych, który powołał administratora bezpieczeństwa informacji i zgłosił go Generalnemu Inspektorowi Ochrony Danych osobowych do rejestracji.

3) dopełnienie obowiązku informacyjnego ustanowionego w art. 24 ust. 1 oraz art. 25 ust. 1 u.o.d.o.;

4) dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą;

5) respektowanie prawa osób, których dane dotyczą;

6) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności do zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym,

zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

7) wydawanie i odbieranie upoważnień do przetwarzania danych;

8) prowadzenie ewidencji wydanych upoważnień do przetwarzania danych osobowych;

9) podejmowanie działań w przypadku wykrycia naruszeń w systemie bezpieczeństwa danych osobowych;

10) kontrolowanie, jakie dane, kiedy i przez kogo zostały wprowadzone do zbioru i komu są przekazywane;

11) udzielanie informacji o zakresie przetwarzanych danych osobowych;

12) spełnienie obowiązku uzupełniania, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane;

13) zapewnienie środków finansowych niezbędnych do ochrony danych osobowych.

7. Powołanie, rejestracja, zmiana i odwołanie Administratora Bezpieczeństwa Informacji.

1) Administrator Danych Osobowych może powołać administratora bezpieczeństwa informacji **(Załącznik Nr 1).**,

2) Administratorem Bezpieczeństwa Informacji może być osoba, która:

2.1) ma pełną zdolność do czynności prawnych oraz korzystania z pełni praw publicznych,

2.2) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych,

2.3) nie była karana za umyślne przestępstwo.

3) Administrator danych jest obowiązany zgłosić do rejestracji Generalnemu Inspektorowi powołanie i odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od dnia jego powołania lub odwołania.

4) Zgłoszenie powołania administratora bezpieczeństwa informacji do rejestracji powinno zawierać:

4.1) oznaczenie administratora danych i adres jego siedziby lub zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany;

4.2) dane administratora bezpieczeństwa informacji:

a) imię i nazwisko,

b) numer PESEL lub, gdy ten numer nie został nadany, nazwę i numer dokumentu stwierdzającego tożsamość,

c) adres do korespondencji, jeżeli jest inny niż adres o którym mowa w pkt.4.1),

4.3) datę powołania,

4.4) oświadczenie administratora danych o spełnieniu przez administratora bezpieczeństwa informacji warunków określonych w pkt 2).

5) Wzory zgłoszeń powołania, zmiany informacji objętych zgłoszeniem i odwołania administratora bezpieczeństwa informacji do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, określają załączniki do Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. 2014, poz. 1934).

6) Administrator danych jest obowiązany zgłosić Generalnemu Inspektorowi zmianę informacji objętych zgłoszeniem, o którym mowa w pkt 4), w terminie do 14 dni od dnia zmiany. Do zgłaszania zmian stosuje się odpowiednio przepisy o zgłoszeniu powołania administratora bezpieczeństwa informacji.

7) Administrator danych może powierzyć administratorowi bezpieczeństwa informacji wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań określonych w pkt. 8. Administrator Bezpieczeństwa Informacji.

8) Administrator danych może powołać zastępców administratora bezpieczeństwa informacji, którzy spełniają warunki określone w pkt. 2).

9) Administrator Bezpieczeństwa Informacji podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej Administratorem Danych.

10) W przypadku niepowołania administratora bezpieczeństwa informacji zadania określone w pkt. 8. Administrator Bezpieczeństwa Informacji, z wyłączeniem obowiązku sporządzenia sprawozdania, wykonuje administrator danych.

8. Administrator Bezpieczeństwa Informacji

Administrator Bezpieczeństwa Informacji odpowiedzialny jest za:

1) prowadzenie dokumentacji dotyczącej bezpieczeństwa danych osobowych;
2) prowadzenie i nadzorowanie korespondencji z Generalnym Inspektorem Ochrony Danych Osobowych;
3) prowadzenie jawnego rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów o których mowa w art. 43 ust. 1,
4) opracowanie sprawozdania z sprawdzenia wykonywanego na wniosek Generalnego Inspektora u administratora danych, który go powołał. Zawartość sprawozdania określa art. 36c. u.o.d.o.;
5) prowadzenie ewidencji zbiorów danych osobowych przetwarzanych w Urzędzie Gminy;
6) prowadzenie wykazu obszarów przetwarzania danych osobowych w Urzędzie Gminy;
7) wydawanie i odbieranie upoważnień do przetwarzania danych;
8) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
9) sprawowanie nadzoru nad prawidłowym stosowaniem się do zasad i procedur określonych w Polityce Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Gminy Masłów;
10) sprawowanie nadzoru nad fizycznym zabezpieczeniem obszarów przetwarzania danych osobowych oraz kontrolę przebywających w nich osób;
11) sprawowanie nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
12) sprawowanie nadzoru nad bezpieczeństwem danych osobowych zawartych na dyskach wymiennych, palmtopach, pamięciach przenośnych i innych nośnikach, a także w komputerach przenośnych;

13) sprawowanie nadzoru nad instalacjami i konfiguracjami oprogramowania systemowego, sieciowego oraz bazodanowego;

14) sprawowanie nadzoru nad profilaktyką antywirusową;

15) sprawowanie nadzoru w zakresie wykonywanych kopii zapasowych danych osobowych;

16) sprawowanie nadzoru nad obiegiem oraz przechowywaniem dokumentacji zawierającej dane osobowe;

17) sprawowanie nadzoru nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemach informatycznych Urzędu Gminy oraz kontrolę dostępu do danych;

18) identyfikowanie i analizowanie zagrożeń oraz ryzyka, na które narażone mogą być dane osobowe przetwarzane w Urzędzie Gminy;

19) monitorowanie działania zabezpieczeń wdrożonych w celu ochrony danych osobowych;

20) przeprowadzanie kontroli w zakresie ochrony danych osobowych;

21) określanie potrzeb w zakresie zabezpieczenia danych osobowych ;

22) aktualizacje jawnego rejestru zbiorów danych osobowych przetwarzanych przez Urząd Gminy;

23) podejmowanie odpowiednich działań w przypadkach naruszenia bezpieczeństwa danych osobowych;

24) prowadzenie rejestru incydentów i zdarzeń wskazujących na naruszenie bezpieczeństwa danych osobowych;

25) zatwierdzanie procedur bezpieczeństwa i standardów zabezpieczeń wnioskowanych i obowiązujących w Urzędzie Gminy;

26) dokonywanie modyfikacji i akceptacji proponowanych zmian, jak i okresowych kontroli polityk i procedur;

27) umożliwienie przeprowadzenia kontroli przez służby Biura Generalnego Inspektora Ochrony Danych Osobowych;

28) sprawowanie nadzoru nad procesem przyznawania praw dostępu;

29) organizowanie szkoleń z zakresu ochrony danych osobowych;

30) opiniowanie zakupów nowych systemów informatycznych;

31) opiniowanie wzorów dokumentów i umów;

32) nadzorowanie Administratora Systemów Informatycznych;

33) nadzorowanie osób upoważnionych do przetwarzania danych osobowych;

34) prowadzenie aktualnego wykazu zbiorów danych osobowych;

35) prowadzenie metryczek zbiorów danych osobowych;

36) zapewnienie, aby dane osobowe prowadzone zbiorach były:

   a) przetwarzane zgodnie z prawem,

   b) zbierane dla oznaczonych i zgodnych z prawem celów,

   c) merytorycznie poprawne i adekwatne w stosunku do celu w jakich są przetwarzane,

   d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą;

37) przygotowywanie wniosków zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych osobowych;

38) prowadzenie aktualnego wykazu budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;

39) zapewnienie poufności, integralności i rozliczalności danych osobowych;

40) określenie indywidualnych obowiązków i odpowiedzialności osób upoważnionych do przetwarzania danych osobowych;

41) sprawowanie nadzoru nad prawidłowym stosowaniem się do zasad i procedur określonych w Polityce Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemami Informatycznymi;

42) zapewnienie szkoleń osobom, które będą dopuszczone do przetwarzania danych osobowych;

43) dopuszczanie do przetwarzania danych osobowych wyłącznie osób upoważnionych do przetwarzania danych osobowych;

44) sprawowanie nadzoru nad właściwym eksploatowaniem systemów informatycznych;

45) sprawowanie nadzoru nad obiegiem oraz przechowywaniem dokumentacji zawierającej dane osobowe;

9. Administrator Systemów Informatycznych

Administrator Systemów Informatycznych odpowiedzialny jest za:

1) bieżący nadzór oraz zapewnienie ciągłości działania systemów informatycznych;

2) optymalizację wydajności systemów informatycznych;

3) zabezpieczenie systemów informatycznych;

4) zarządzanie konfiguracją systemów i urządzeń wchodzących w skład systemu informatycznego;

5) przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych w systemach informatycznych;

6) dokonywanie okresowej analizy ryzyka dla poszczególnych systemów informatycznych wykorzystywanych do przetwarzania danych osobowych;

7) prowadzenie dokumentacji systemowej opisującej działania związane z administracją systemów informatycznych, w których przetwarzane są dane osobowe;

8) przyznawanie na wniosek Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do systemów informatycznych;

9) współpracę z dostawcami aplikacji i sprzętu komputerowego w tym sieciowego i serwerowego;

10) wnioskowanie do Administratora Bezpieczeństwa Informacji w sprawie procedur bezpieczeństwa i standardów zabezpieczeń;

11) opracowywanie procedur dotyczących bezpieczeństwa i standardów zabezpieczeń w systemach informatycznych;

12) udostępnianie danych zgromadzonych w systemach informatycznych na wniosek Administratora Danych Osobowych oraz za zgodą Administratora Bezpieczeństwa Informacji;

13) bieżące wykonywanie kopii systemowych jak i kopii baz danych i aplikacji wykorzystywanych do przetwarzania danych osobowych;

14) świadczenie wsparcia technicznego w ramach oprogramowania oraz serwis sprzętu komputerowego wchodzącego w skład systemów informatycznych Urzędu Gminy;

15) diagnozowanie i usuwanie awarii sprzętu komputerowego oraz utrzymywanie kontaktu z firmami świadczącymi usługi pogwarancyjne sprzętu komputerowego;

16) prowadzenie dokumentacji dotyczącej opisu struktury zbiorów danych osobowych oraz udostępnianie jej Administratorowi Bezpieczeństwa Informacji;

17) prowadzenie dokumentacji dotyczącej opisu przepływu danych pomiędzy systemami informatycznymi zastosowanymi w celu przetwarzania danych osobowych oraz udostępnianie jej Administratorowi Bezpieczeństwa Informacji;

18) prowadzenie ewidencji sprzętu i oprogramowania służącego do przetwarzania danych osobowych;

umożliwienie przeprowadzenia kontroli przez służby Biura Generalnego Inspektora Ochrony Danych Osobowych;

19) sprawowanie nadzoru nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji;

20) wykonywanie napraw oraz konserwacji systemów informatycznych a także likwidację urządzeń komputerowych oraz elektronicznych nośników zawierających dane osobowe;

21) sprawowanie nadzoru nad bezpieczeństwem danych osobowych zawartych na dyskach wymiennych, palmtopach, pamięciach przenośnych i innych nośnikach, a także w komputerach przenośnych;

22) sprawowanie nadzoru nad profilaktyką antywirusową;

23) zapewnienie szkoleń Pracowników Urzędu w zakresie prawidłowego korzystania z aplikacji i urządzeń wchodzących w skład systemów informatycznych służących do przetwarzania danych osobowych;

24) opiniowanie zakupów dotyczących urządzeń sieciowych i serwerowych;

25) opiniowanie zakupów dotyczących oprogramowania sieciowego, serwerowego oraz narzędziowego;

10. Osoby odpowiedzialne za przetwarzanie danych osobowych

Osoby upoważnione do przetwarzania danych osobowych odpowiedzialne są za:

1) zapoznanie się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej Polityki Bezpieczeństwa Danych Osobowych i Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Gminy Masłów;
2) stosowanie się do zaleceń Administratora Bezpieczeństwa Informacji oraz Administratora Systemów Informatycznych w zakresie ich kompetencji;
3) przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych w pisemnym upoważnieniu i tylko w celu wykonywania nałożonych obowiązków służbowych;
4) niezwłoczne informowanie Administratora Bezpieczeństwa Informacji o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy;
5) ochronę danych osobowych oraz środków wykorzystywanych do przetwarzania danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
6) korzystanie z systemów informatycznych Urzędu Gminy w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemów informatycznych;
7) zachowanie w tajemnicy danych osobowych oraz przestrzegania procedur ich bezpiecznego przetwarzania przez cały okres zatrudnienia, a także po ustaniu stosunku pracy lub odwołania z pełnionej funkcji;
8) wszelkie operacje wykonywane w systemach informatycznych przy użyciu ich identyfikatora oraz hasła;
9) zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów osób, których dane dotyczą.

11. Podstawowe zasady ochrony danych osobowych

1) Wszystkie dane osobowe w Urzędzie Gminy Masłów należy przetwarzać zgodnie z obowiązującymi przepisami prawa;
2) W stosunku do osób, których dane osobowe są przetwarzane należy spełnić obowiązek informacyjny wynikający z przepisów u.o.d.o.;
3) Zebrane dane osobowe należy przetwarzać dla oznaczonych i zgodnych z prawem celów i nie poddawać dalszemu przetwarzaniu niezgodnemu z tymi celami;
4) Należy zadbać, aby przetwarzanie danych osobowych odbywało się zgodnie z zasadami dotyczącej merytorycznej poprawności oraz adekwatnie do celów w jakich zostały zebrane;
5) Przetwarzane dane osobowe należy przechowywać w postaci umożliwiającej identyfikację osób, których te dane dotyczą;
6) Dane osobowe w Urzędzie Gminy można przetwarzać nie dłużej niż jest to niezbędne do osiągnięcia celu ich przetwarzania;
7) Należy zapewnić poufność, integralność oraz rozliczalność danych osobowych przetwarzanych w Urzędzie Gminy;
8) Przetwarzane dane osobowe nie mogą być udostępniane bez zgody osób, których dane dotyczą, chyba że udostępnia się te dane osobom, których dane dotyczą, osobom upoważnionym do przetwarzania danych osobowych, podmiotom którym przekazano dane na podstawie umowy powierzenia oraz organom państwowym lub organom samorządu terytorialnego w związku z prowadzonym postępowaniem;
9) Przetwarzanie danych osobowych w Urzędzie Gminy może odbywać się zarówno w systemach informatycznych, jak i w formie tradycyjnej: kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych;
10) W zakresie danych osobowych przetwarzanych w innych systemach niż informatyczne, obowiązują nadal dotychczasowe przepisy o tajemnicy służbowej, obiegu i zabezpieczaniu dokumentów służbowych;
11) Wszystkim osobom, których dane są przetwarzane przysługuje prawo do ochrony danych ich dotyczących, do kontroli przetwarzania tych danych oraz do ich uaktualniania, usunięcia jak również do uzyskiwania wszystkich informacji o przysługujących im prawach.

12. Upoważnienia do przetwarzania danych osobowych

Do przetwarzania danych osobowych oraz obsługi zbiorów informatycznych zawierających te dane mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez Administratora Bezpieczeństwa Informacji z upoważnienia Administratora Danych Osobowych. Upoważnienie wydaje się na wniosek Kierownika Komórki Organizacyjnej, osobie która złożyła stosowne oświadczenie dot. właściwej realizacji przepisów u.o.d.o.

Upoważnienie powinno mieć charakter imienny. Powinno też określać dozwolony okres i zakres przetwarzania danych. Upoważnienia mogą być wydawane bezterminowo (wynikające z treści umowy o pracę) lub na czas określony.

Procedura nadawania upoważnienia do przetwarzania danych osobowych:

1) W przypadku przyjęcia do pracy nowego pracownika, którego zakres obowiązków obejmować będzie przetwarzanie danych osobowych, Kierownik Komórki Organizacyjnej zobowiązany jest zwrócić się do Administratora Bezpieczeństwa Informacji na wniosku (wzór wniosku stanowi **Załącznik Nr 2**) o wydanie upoważnienia do przetwarzania danych osobowych.

2) W przypadku zmiany stanowiska, bądź zakresu obowiązków pracowniczych, lub w sytuacji, która wpływa bezpośrednio na rodzaj i zakres przetwarzanych danych osobowych, przełożony lub osoba pełniąca samodzielne stanowisko zobowiązani są bezzwłocznie skierować wniosek (wzór wniosku stanowi **Załącznik Nr 2**) do Administratora Bezpieczeństwa Informacji o wydanie lub cofnięcie upoważnienia.

3) Nowy pracownik podpisuje oświadczenie (wzór oświadczenia stanowi **Załącznik Nr 3**) dot. właściwej realizacji przepisów u.o.d.o.

3) Administrator Danych Osobowych wydaje upoważnienie (wzór upoważnienia stanowi **Załącznik Nr 4**) do przetwarzania danych osobowych po spełnieniu procedury określonej w ust. 1 i 2 oraz 3.

4) Rozwiązanie stosunku pracy powoduje wygaśnięcie upoważnienia.

5. Ewidencję pracowników, upoważnionych do przetwarzania danych osobowych prowadzi Administrator Bezpieczeństwa Informacji (wzór ewidencji stanowi **Załącznik Nr 5**).

13. Powierzenie przetwarzania danych osobowych

Administrator Danych Osobowych może zlecić innemu podmiotowi przetwarzanie danych osobowych w celu realizacji określonego zadania.

W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim:

a) cel i zakres przetwarzania danych osobowych;

b) obowiązek zachowania w tajemnicy danych osobowych oraz informacji o zabezpieczeniach tych danych;

c) konsekwencje prawne i kary finansowe wynikające z niestosowania się do warunków umowy;

d) wymagania bezpieczeństwa dla procesu przetwarzania danych osobowych.

W umowach powierzenia przetwarzania danych osobowych oraz w umowach, na podstawie, których dochodzi do wymiany informacji uwzględnić należy następujące elementy:

a) definicje informacji, która ma być chroniona;

b) spodziewany czas trwania umowy, włączając w to przypadki, w których obowiązek zachowania poufności może być bezterminowy;

c) odpowiedzialność i działania sygnatariuszy podejmowane w celu uniknięcia nieupoważnionego ujawnienia informacji;

d) własność informacji;

e) dozwolone użycie danych osobowych oraz praw sygnatariusza do jej użycia;

f) prawa do audytu i monitorowania działań związanych z ochrona danych osobowych;

g) proces powiadamiania i raportowania nieuprawnionego ujawnienia lub naruszenia poufności i integralności danych osobowych;

h) wymagane działania w momencie zakończenia umowy, np.: zasady zwrotu lub niszczenia danych osobowych przy zakończeniu umowy.

Powierzenie przetwarzania danych osobowych poza granice Rzeczpospolitej Polskiej wymaga zgody Administratora Danych Osobowych i odbywa się po sprawdzeniu wymagań prawnych obowiązujących w tym zakresie.

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

Administrator Bezpieczeństwa Informacji odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji opisującej obszar przetwarzania danych osobowych w siedzibie Urzędu Gminy Masłów który stanowią pomieszczenia, w których przetwarzane są dane osobowe z użyciem sprzętu komputerowego lub w formie kartotek, skorowidzów, ksiąg, wykazów i innych zbiorów ewidencyjnych.

Dokumentacja ta stanowi część Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy Masłów, prowadzona jest zgodnie ze wzorcem (wzór wykazu stanowi **Załącznik Nr 6**).

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

Administrator Bezpieczeństwa Informacji odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej wykaz wszystkich zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Dokumentacja ta stanowi część Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Masłów, prowadzona jest zgodnie ze wzorem (wzór wykazu stanowi **Załącznik Nr 7**).

Wykaz zbiorów prowadzony jest zarówno w formie papierowej jak i elektronicznej.

16. Opis struktury zbiorów

Administrator Bezpieczeństwa Informacji odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej opis struktury zbiorów danych osobowych przetwarzanych w Urzędzie Gminy Masłów. Dokumentacja opracowana została w oparciu o materiały dostarczone przez producentów oprogramowania i prowadzona jest w konsultacji z Administratorem Systemów

Informatycznych. Dokumentacja prowadzona jest zgodnie ze wzorem (wzór opisu stanowi **Załącznik Nr 8**).

Dokumentacja ta stanowi część Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Masłów. Prowadzona jest zarówno w formie papierowej jak i elektronicznej.

17. Opis sposobu przepływu danych pomiędzy poszczególnymi systemami.

Administrator Systemów Informatycznych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej opis sposobu przepływu danych pomiędzy poszczególnymi systemami. Dokumentacja ta stanowi część Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Masłów. Dokumentacja prowadzona jest zarówno w formie papierowej jak i elektronicznej. Wszelkie zmiany ww. dokumencie są opiniowane i zatwierdzane przez Administratora Bezpieczeństwa Informacji.

18. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Środki ochrony fizycznej

- obszar, w którym przetwarzane są dane osobowe po godzinach pracy urzędu chroniony jest alarmem;
- obszar, w którym przetwarzane są dane osobowe całodobowo jest monitorowany wizyjnie z miesięczną rejestracją oraz jest nadzorowany przez pracowników ochrony;
- wszystkie pomieszczenia w których przetwarzane są dane osobowe są zamykane na klucz w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych – także w godzinach pracy;
- przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych jest możliwy tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności kierownika referatu.
- Dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pendrive, płyta CD/DVD, dyskietka) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam gdzie jest to możliwe – w szafach metalowych lub pancernych. Klucze do szafek należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych;
- Ustawianie monitorów stanowisk przetwarzania danych osobowych w sposób uniemożliwiający wgląd w dane osobom nieupoważnionym.

Środki sprzętowe, informatyczne i telekomunikacyjne

- Nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach;
- sieć lokalna jest podłączona do Internetu za pomocą komputera spełniającego funkcję Servera Proxy oraz Firewalla;
- wszystkie stanowiska komputerowe wyposażone są w indywidualną ochronę antywirusową;
- wszystkie stanowiska komputerowe oraz serwery są chronione przed zanikiem zasilania przez stosowanie zasilaczy zapasowych UPS;
- kopie awaryjne wykonuje się na płytach DVD-R, zapisuje się je również na serwerze plików,
- każdy komputer zabezpieczony jest przez indywidualny identyfikator użytkownika i cyklicznie zmieniane hasło;
- podłączenie urządzenia końcowego (komputera, drukarki) do sieci lokalnej dokonywane jest przez Administratora Systemu Informatycznego.

Środki ochrony w ramach oprogramowania systemu

- ile istnieje taka możliwość, w systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę hasła dostępu do systemu;
- ile istnieje taka możliwość, zastosowano identyfikator i hasło dostępu na poziomie aplikacji;
- konfiguracja systemu umożliwia użytkownikom dostęp do danych osobowych jedynie za pośrednictwem aplikacji;
- system informatyczny pozwala zdefiniować odpowiednie prawa do zasobów informatycznych systemu.

Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych

- zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji;
- dla każdego użytkownika systemu nadawany jest odrębny identyfikator;

Środki organizacyjne

- wyznaczono Administratora Bezpieczeństwa Informacji,
- osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do tych danych szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych oraz procedur przetwarzania danych;
- prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,
- ustalono instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
- zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych;
- zapoznano i zobowiązano na piśmie pracowników urzędu do przestrzegania przepisów i zasad związanych z bezpieczeństwem przetwarzania danych osobowych.

19. Archiwizowanie informacji zawierających dane osobowe

Zasady archiwizowania informacji zawierających dane osobowe w Urzędzie Gminy Masłów regulują następujące przepisy:

1) Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. 2011 nr 123 poz. 698)
2) Rozporządzenie Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz.U. 2002 nr 167 poz. 1375)
3) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 2 listopada 2006 r. w sprawie wymagań technicznych formatów zapisu i informatycznych nośników danych, na których utrwalono materiały archiwalne przekazywane do archiwów państwowych (Dz. U. Nr 206, poz. 1519);
4) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz. U. Nr 206, poz. 1518);
5) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz. U. Nr 206, poz. 1517);

20. Instrukcja alarmowa w przypadku wystąpienia zagrożenia lub incydentu naruszającego ochronę danych osobowych

Celem Instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń oraz występowania incydentów w przyszłości. Poniższe zasady postępowania mają zastosowanie zarówno w przypadku danych osobowych przetwarzanych w formie tradycyjnej (kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych) jak i w systemach informatycznych Urzędu Gminy.

Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

1) brak lub niewłaściwe zabezpieczenia fizyczne pomieszczeń, urządzeń i dokumentów;

2) brak lub niewłaściwe zabezpieczenie sprzętu IT oraz oprogramowania przed wyciekiem, kradzieżą lub utratą danych osobowych;

3) niestosowanie zasad ochrony danych osobowych przez osoby upoważnione w tym:

   a) nieprzestrzeganie zasad czystego biurka i ekranu,
   b) ochrony haseł,

c) niezamykanie pomieszczeń, szafek, biurek itp.

Do typowych incydentów bezpieczeństwa danych osobowych należą:

a) zdarzenia losowe zewnętrzne:
   - pożar obiektu lub pomieszczenia,
   - zalanie wodą,
   - utrata zasilania,
   - utrata łączności itp.;

b) zdarzenia losowe wewnętrzne
   - awarie sprzętu komputerowego lub oprogramowania,
   - pomyłki Administratora Systemów Informatycznych lub osób upoważnionych,
   - utrata/zagubienie nośników zawierających dane osobowe itp.;

c) umyślne incydenty:
   - nieuprawniony dostęp do systemów informatycznych lub pomieszczeń (włamanie),
   - wyciek danych osobowych,
   - ujawnienie danych osobowych osobom nieupoważnionym,
   - działanie wirusów lub innego szkodliwego oprogramowania,
   - świadome zniszczenie danych,
   - kradzież danych itp.

Przed przystąpieniem do pracy osoby upoważnione zobowiązane są do zwrócenia szczególnej uwagi, czy nie zaszły okoliczności wskazujące na wystąpienie zagrożenia lub incydentu naruszającego ochronę danych osobowych.

W przypadku stwierdzenia zagrożenia lub incydentu naruszenia ochrony danych osobowych, należy niezwłocznie poinformować o tym fakcie Administratora Bezpieczeństwa Informacji. W sytuacji braku możliwości zawiadomienia Administratora Bezpieczeństwa Informacji należy powiadomić Sekretarza Gminy.

Informację o pojawieniu się zagrożenia lub incydentu należy przekazać osobiście lub telefonicznie. Informacja ta powinna zawierać imię i nazwisko osoby zgłaszającej, miejsce i czas wystąpienia zagrożenia lub incydentu oraz krótki opis sytuacji. Osoba zgłaszająca wystąpienie zagrożenia lub incydentu może zostać poproszona o potwierdzenie zgłoszenia na piśmie.

Do czasu przybycia Administratora Bezpieczeństwa Informacji lub Sekretarza Gminy, zgłaszający:

a) Powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również do podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów;

b) Zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym;

c) Podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

Dokonywanie zmian w miejscu wystąpienia zagrożenia lub incydentu jest dopuszczalne w przypadku, gdy zachodzi konieczność ratowania osób lub mienia albo zapobieżenia wystąpienia niebezpieczeństwa.

W sytuacji stwierdzenia wystąpienia zagrożenia lub incydentu zagrażającemu bezpieczeństwu danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od Administratora Bezpieczeństwa Informacji lub Sekretarza Gminy. W przypadku, gdy zagrożenie lub incydent jest wynikiem uchybienia obowiązującej w firmie dyscypliny pracy, Administrator Bezpieczeństwa Informacji wyjaśnia wszystkie okoliczności zaistniałej sytuacji i podejmuje stosowne działania wobec osób, które dopuściły się wskazanego naruszenia.

Po zakończeniu czynności naprawczych system powinien utrzymać poziom ochrony nie niższy niż przed wystąpieniem zagrożenia lub incydentu związanego z naruszeniem ochrony danych osobowych.

Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia rejestru incydentów i zdarzeń wskazujących na naruszenie bezpieczeństwa danych osobowych. Rejestr incydentów prowadzony jest zgodnie ze wzorem (wzór rejestru **Załącznik Nr 9**).

21. Działania korygujące i zapobiegawcze

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych. Źródłami informacji o incydentach, zagrożeniach lub słabościach są:

a) zgłoszenia od pracowników;

b) wyniki kontroli.

W przypadku, gdy Administrator Bezpieczeństwa Informacji stwierdza konieczność podjęcia działań korygujących lub zapobiegawczych, określa:

a) źródło powstania incydentu lub zagrożenia;

b) zakres działań korygujących lub zapobiegawczych;

c) termin realizacji;

d) osobę odpowiedzialną.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad poprawą i terminowością wdrażanych działań korygujących lub zapobiegawczych.

Po wprowadzeniu działań korygujących lub zapobiegawczych, Administrator Bezpieczeństwa Informacji jest zobowiązany do oceny efektywności ich zastosowania.

22. Przepisy karne i porządkowe

Wobec osoby, która w przypadku naruszenia zasad ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działań określonych w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiednich osób zgodnie z określonymi zasadami, można wszcząć postępowanie dyscyplinarne.

Osoba upoważniona dopuszczająca się nieuprawnionego ujawniania lub wykorzystywania danych osobowych w sposób sprzeczny z ich przeznaczeniem, czy też ich przetwarzania w sposób niezgodny z przyjętymi w Urzędzie Gminy Masłów zasadami i procedurami, może zostać ukarany karą upomnienia lub karą nagany.

Naruszenie zasad ochrony danych osobowych przez osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych może skutkować postawieniem zarzutu popełnienia jednego z przestępstwa określonych w Rozdziale 8 u.o.d.o. lub przestępstwa określonego w art. 266 Kodeksu Karnego.

Przepisy karne i porządkowe reguluje:

1) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.) - art. 49-54;

2) ustawa z dnia 6 czerwca 1997 r. Kodeks Karny (Dz. U. z 1997 r., Nr 88, poz. 553, z późn. zm.) - art. 266;

3) ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 1998 r., Nr 21, poz. 94, z późn. zm.) - art. 52 oraz art. 108;

4) ustawa z dnia 21 listopada 2008 r. o pracownikach samorządowych (Dz. U. z 2008 r., Nr 223, poz. 1458, z późn. zm.);

23. 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, potwierdzające znajomość jego treści oraz odbycia szkolenia w zakresie bezpieczeństwa danych osobowych.

Polityka Bezpieczeństwa Danych Osobowych jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie za wyjątkiem osób upoważnionych do przetwarzania danych osobowych w Urzędzie Gminy Masłów.

W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa Danych Osobowych mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t.j. Dz.U. 2014 r. poz. 1182 z późn. zm.) oraz przepisy wykonawcze do tej Ustawy.

24. Spis wzorów dokumentów

Załącznik Nr 1 – Wzór powołania Administratora Bezpieczeństwa Informacji.

Załącznik Nr 2 – Wzór wniosku o nadanie upoważnienia do przetwarzania danych osobowych.

Załącznik Nr 3 – Wzór oświadczenia.

Załącznik Nr 4 – Wzór upoważnienia do przetwarzania danych osobowych.

Załącznik Nr 5 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych.

Załącznik Nr 6 – Wzór wykazu pomieszczeń.

Załącznik Nr 7 – Wzór wykazu zbiorów.

Załącznik Nr 8 – Wzór opisu struktury zbiorów

Załącznik Nr 9 – Wzór rejestru *incydentów*.

WÓJT
mgr Tomasz Lato

URZĄD GMINY MASŁÓW
ul. Spokojna 2, 26-001 Masłów
REG.000547313, NIP 657 17 48 114

Urząd Gminy Masłów
Załącznik Nr 1 (wzór)

Powołanie na stanowisko Administratora Bezpieczeństwa Informacji

Na podstawie art. 36a ust. 1 Ustawy o Ochronie Danych Osobowych z 29 sierpnia 1997 roku (Dz. U. z 2014 r. poz. 1182, z późn. zm.), z dniem ..... wyznaczam:

Panią/Pana

.....

/Imię i Nazwisko/

na

ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Zakres zadań, upoważnień i odpowiedzialności Administratora Bezpieczeństwa Informacji określa Polityka Bezpieczeństwa Danych Osobowych.

Administrator Danych Osobowych	**Administrator Bezpieczeństwa Informacji**
.....	.....
/data, pieczęć i podpis ADO/	/data i podpis ABI/

WÓJT
mgr Tomasz Lato

URZĄD GMINY MASŁÓW
ul. Spokojna 2, 26-001 Masłów
REG.000547313, NIP 657 17 48 114

Urząd Gminy Masłów
Załącznik Nr 2 (wzór)

Wniosek o wydanie, zmianę, cofnięcie upoważnienia

W związku z: (należy zaznaczyć odpowiednie pole):

Zatrudnienie nowego pracownika	Zmiana stanowiska	Zmiana zakresu obowiązków
☐	☐	☐
Tworzenie nowego zbioru danych	**Inne**	**Inne (opis)**
☐	☐	

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych proszę o wydanie / cofnięcie / zmianę (upoważnienia z dnia .....) do przetwarzania danych osobowych wynikających z zakresu obowiązków pracowniczych dla:

Imię:	Nazwisko:
Stanowisko:	**Komórka:**

Opis zakresu uprawnień:

Data i podpis wnioskodawcy

WÓJT
mgr Tomasz Lato

Urząd Gminy Masłów
Załącznik Nr 3 (wzór)

Oświadczenie
osoby dopuszczonej do przetwarzania danych osobowych

Ja niżej podpisana/ny oświadczam, że:

1. przed przystąpieniem do pracy przy przetwarzaniu danych osobowych zostałam/em zaznajomiona/y z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r. poz. 1182, z późn. zm.) oraz rozporządzeniami wykonawczymi wydanymi na jej podstawie,
2. zapoznałam/em się i rozumiem zasady dotyczące ochrony danych osobowych opisane w:
    - Polityce Bezpieczeństwa
    - Instrukcji Zarządzania Systemem Informatycznym

    oraz zobowiązuję się do ich przestrzegania,
3. uczestniczyłam/em w szkoleniu z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w Urzędzie Gminy Masłów.
4. Ponadto zobowiązuję się zachować w tajemnicy dane osobowe, które będę przetwarzać oraz znane mi sposoby zabezpieczenia danych osobowych stosowane w Urzędzie Gminy Masłów, przez cały okres zatrudnienia u Administratora Danych Osobowych / świadczenia usług na rzecz Administratora Danych Osobowych*, również po ustaniu zatrudnienia / zakończenia świadczenia usług na rzecz Administratora Danych Osobowych*, do momentu ich upublicznienia.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane za naruszenie przepisów karnych ustawy dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r. poz. 1182, z późn. zm.).

.....

/podpis składającego oświadczenie/

* niepotrzebne skreślić

WÓJT
inż. Tomasz Lato

URZĄD GMINY MASŁÓW
ul. Spokojna 2, 26-001 Masłów
REG.000547313, NIP 657 17 48 114

Urząd Gminy Masłów
Załącznik Nr 4 (wzór)

Upoważnienie nr .....
do przetwarzania danych osobowych

Na podstawie art. 37 Ustawy o Ochronie Danych Osobowych z 29 sierpnia 1997 roku (Dz. U. z 2014 r. poz. 1182 z późn. zm.), upoważniam Panią/Pana:

.....

/Imię i Nazwisko/

zatrudnioną/-nego na stanowisku: .....

do przetwarzania od dnia ..... r. danych osobowych w następującym zakresie:

- wykonywanie obowiązków służbowych na stanowisku pracy i poleceń przełożonego*

- wykonywanie obowiązków zleceniobiorcy*

i w systemie informatycznym nadaję identyfikator: .....

Niniejsze upoważnienie jest ważne w okresie od ..... do

.....

Administrator Danych Osobowych

.....

/podpis/

* niepotrzebne skreślić

WÓJT
mgr Tomasz Lato

URZĄD GMINY MASŁÓW
ul. Spokojna 2, 26-001 Masłów
REG.000547313, NIP 657 17 48 114

Urząd Gminy Masłów
Załącznik Nr 5 (wzór)

Ewidencja osób upoważnionych do przetwarzania danych osobowych.

Lp.	Imię i Nazwisko, zajmowane stanowisko /data zmiany danych	Identyfikator w systemie informatycznym*	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania upoważnienia	Data ustania upoważnienia
1	2	3	4	5	6
1					
	Zmiana danych**				
2					
	Zmiana danych**				

* Identyfikator jest wymagany jeśli dane są przetwarzane w systemie informatycznym.

** W przypadku zmiany danych wypełnić należy te rubryki, których zmiany dotyczą – pozostałe należy przekreślić.

WÓJT
mgr Tomasz Lato

URZĄD GMINY MASŁÓW
ul. Spokojna 2, 26-001 Masłów
REG.000547313, NIP 657 17 48 114

Urząd Gminy Masłów
Załącznik Nr 6 (wzór)

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

Lp.	Miejsce przetwarzania danych osobowych /adres/	Obszar przetwarzania danych osobowych /nazwa pomieszczenia, nr itp./
1	2	3
1		

WÓJT
mgr Tomasz Lato

URZĄD GMINY MASŁÓW
ul. Spokojna 2, 26-001 Masłów
REG.000547313, NIP 657 17 48 114

Urząd Gminy Masłów
Załącznik Nr 7 (wzór)

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

Lp.	Zbiór danych osobowych	Zastosowany program do przetwarzania danych
1	2	3
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

WÓJT
mgr Tomasz Lato

URZĄD GMINY MASŁÓW
ul. Spokojna 2, 26-001 Masłów
REG.000547313, NIP 657 17 48 114

Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Zbiór danych osobowych	Opis struktury zbioru
2	3

WÓJT
mgr Tomasz Lato

Urząd Gminy Masłów
Załącznik Nr 9 (wzór)

Ewidencja incydentów bezpieczeństwa i działań korygujących oraz zapobiegawczych.

L.p.	Incydent/zadanie /problem	Źródło zgłoszenia	Data rozpoczęcia	Data zakończenia	Odpowiedzialny za realizację	Przyczyna niezgodności	Działania korygujące /zapobiegawcze	Ocena skuteczności

WÓJT
mgr Tomasz Lato

Załącznik nr. 2 do Zarządzenia nr 183//2015
Wójta Gminy Masłów
z dnia 05.11.2015 roku

Instrukcja Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych

Urzędu Gminy Masłów

Urząd Gminy
Masłów

26-001 Masłów
Spokojna 2
Powiat Kielecki
Województwo
Świętokrzyskie

www.maslow.pl
gmina@maslow.pl

Wstęp

Celem wydania dokumentu jest realizacja zapisów „Polityki Bezpieczeństwa" przetwarzania danych osobowych obowiązującej w Urzędzie Gminy Masłów oraz postanowień §5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Spis treści

1. Definicje

Ilekroć w niniejszej Instrukcji Zarządzania Systemem Informatycznym mowa o:

1) **komórce organizacyjnej** – rozumie się przez to odpowiednio wydziały i komórki organizacyjne, o których mowa w Rozdziale III §8 - §16 Regulaminu Organizacyjnego Urzędu Gminy w Masłowie stanowiącego załącznik do Zarządzenia Nr 201/2013 Wójta Gminy Masłów z dnia 31 grudnia 2013 roku.

2) **Kierowniku komórki organizacyjnej** – rozumie się przez to kierownika wydziału, referatu, biura, koordynatora i samodzielne stanowiska pracy;

3) **Administratorze Danych Osobowych** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych. Administratorem Danych Osobowych jest Wójt Gminy Masłów;

4) **Administratorze Bezpieczeństwa Informacji** – rozumie się przez to pracownika Urzędu Gminy wyznaczonego przez Administratora Danych Osobowych, nadzorującego przestrzeganie zasad, o których mowa w art. 36 ust. 1 u.o.d.o.;

5) **Administratorze Systemów Informatycznych** – rozumie się przez to pracownika Urzędu Gminy, odpowiedzialnego za funkcjonowanie systemów i sieci teleinformatycznych oraz za przestrzeganie zasad i wymogów bezpieczeństwa systemów i sieci teleinformatycznych;

6) **Osobie upoważnionej** – rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych. Użytkownikiem może być pracownik Urzędu Gminy, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, a także osoba odbywająca wolontariat, praktykę lub staż.

7) **Osobie nieupoważnionej** – rozumie się przez to osobę nieposiadającą upoważnienia do przetwarzania danych osobowych;

8) **Osobie nieuprawnionej** – rozumie się przez to osobę nieposiadającą uprawnień nadanych w systemie informatycznym Urzędu Gminy;

9) **Danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na

numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość;

10) **Zbiorze danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

11) **Przetwarzaniu danych osobowych** – 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) **Zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

14) **Bezpieczeństwie informacji** – rozumie się przez to zespół zasad, jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania informacji by w każdych okolicznościach dostęp do nich był zgodny z założeniami;

15) **Usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

16) **Zgodzie osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgoda może być odwołana w każdym czasie;

17) **Odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe za wyjątkiem:

    a) osoby, której dane dotyczą,

    b) osoby upoważnionej do przetwarzania danych osobowych,

c) przedstawiciela, o którym mowa w art. 31a u.o.d.o.,

d) podmiotu, o którym mowa w art. 31 u.o.d.o.,

e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

18) **Państwie trzecim** – rozumie się przez to państwo należące do Europejskiego Obszaru Gospodarczego;

19) **Haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi uprawnionemu do pracy w systemie informatycznym;

20) **Identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w wyznaczonych przez Administratora Danych Osobowych obszarach systemu informatycznego Urzędu Gminy;

21) **Teletransmisji danych** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnych;

22) **Poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;

23) **Integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

24) **Rozliczalności danych** – rozumie się przez to właściwość zapewniającą, że działania osoby lub podmiotu mogą być przypisane w sposób jednoznaczny tylko tej osobie lub podmiotowi;

25) **Użytkowniku systemu informatycznego** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych w systemach informatycznych, której nadano unikalny identyfikator i hasło

26) **Uwierzytelnieniu** – rozumie się przez to proces poprawnej identyfikacji użytkownika systemu informatycznego w stopniu umożliwiającym przyznanie odpowiednich uprawnień lub przywilejów w systemie informatycznym Urzędu Gminy;

27) **Sieci komputerowej** – rozumie się przez to grupę komputerów lub innych urządzeń połączonych ze sobą w celu wymiany danych lub współdzielenia różnych zasobów;

28) **Sieci lokalnej** – rozumie się przez to sieć przeznaczoną do łączenia ze sobą stanowisk komputerowych znajdujących się w Urzędzie Gminy;

29) **Sieć publicznej** – rozumie się przez to sieć publiczną w rozumieniu art. 2 ust. 22 ustawy z dnia 21 lipca 2000 r. Prawo telekomunikacyjne (Dz. U. nr 73, poz. 852 z późn. zm.);

30) **Punkcie dystrybucyjnym** – rozumie się przez to miejsce, w którym zlokalizowana jest infrastruktura teleinformatyczna oraz urządzenia umożliwiające dystrybucję połączeń sieciowych w systemie informatycznym Urzędu Gminy;

31) **Stacji roboczej** – rozumie się przez to komputer użytkownika systemu informatycznego podłączony do sieci lokalnej Urzędu Gminy;

32) **Incydent** – rozumie się przez to naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność;

33) **Zagrożenie** - rozumie się przez to potencjalną możliwość wystąpienia incydentu;

34) **Działania korygujące** – rozumie się przez to działanie przeprowadzone w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji;

35) **Działania zapobiegawcze** – rozumie się przez to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej.

1. Wprowadzenie

Instrukcja została opracowana zgodnie z wymogami §5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Niniejsza instrukcja stanowi zestaw procedur opisujących zasady bezpieczeństwa danych osobowych przetwarzanych w zbiorach papierowych oraz w systemach informatycznych Urzędu Gminy Masłów. Instrukcja powstała w celu realizacji zapisów „Polityki Bezpieczeństwa" przetwarzania danych osobowych w Urzędzie Gminy Masłów i jest z nią komplementarna.

2. Zakres stosowania Instrukcji Zarządzania Systemem Informatycznym

Procedury i zasady określone w niniejszym dokumencie powinny być znane i stosowane przez wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemie informatycznym Urzędu Gminy Masłów, bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy.

3. Podstawy prawne

Instrukcja Zarządzania Systemem Informatycznym odnosi się do sposobu przetwarzania danych osobowych oraz środków ich ochrony wraz z określeniem warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do ich przetwarzania, określone w:

1) ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r. poz. 1182, ze zm.)

2) rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r., Nr 100, poz. 1024).

4. Zasady bezpiecznej eksploatacji systemu informatycznego

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

2) W celu zachowania odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych, dostęp do systemu informatycznego powinien być możliwy wyłącznie po podaniu identyfikatora odrębnego dla każdego użytkownika systemu i poufnego hasła lub innego elementu uwierzytelniającego.

3) Należy zapewnić poufność, integralność i rozliczalność danych osobowych przetwarzanych w systemie informatycznym Urzędu Gminy.

4) Należy zapewnić, aby użytkownicy systemu informatycznego służącego do przetwarzania danych osobowych nie posiadali wyższych poziomów uprawnień w tym systemie niż wymagane jest to do wykonywania powierzonych obowiązków.

5) Prawidłowy poziom zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych zostaje zapewniony poprzez przestrzeganie następujących zasad:

a) uniemożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemu informatycznego,

b) niepodejmowanie przez użytkowników systemu prób wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie, a także poprzez instalowanie nowego lub aktualizowanie już zainstalowanego oprogramowania,

c) korzystanie z systemu informatycznego dla celów innych niż związane z wykonywaniem obowiązków służbowych jest zabronione.

6) Dostęp do poszczególnych usług systemu informatycznego powinien być chroniony kontrolą dostępu.

7) Przesyłanie danych osobowych drogą teletransmisji odbywa się wyłącznie przy wykorzystaniu wymaganych zabezpieczeń logicznych chroniących przed nieuprawnionym dostępem, w szczególności takich jak ochrona kryptograficzna.

8) Inne technologie sieciowe takie jak sieci lokalne oparte na falach radiowych nie mogą być wykorzystywane do przekazu informacji, o ile połączenie nie jest szyfrowane. Takie połączenia mogą być używane jedynie dla wymiany poczty elektronicznej o ile wiadomo, że nie zawiera ona danych osobowych.

9) Wszystkie połączenia zewnętrzne do systemu informatycznego powinny być monitorowane, a logi połączeń archiwizowane w trybie ciągłym.

10) Użytkownicy systemu powinni podlegać okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym oraz w związku ze zmiana przepisów o ochronie danych osobowych lub zmiana wewnętrznych regulacji.

5. Zasady przetwarzania danych w zbiorach doraźnych

1) Dostęp do danych osobowych powinien odbywać się poprzez dedykowane aplikacje, działające w architekturze klient-serwer, lub przynajmniej, przechowujące dane na serwerach plików, nie zaś na indywidualnych stanowiskach komputerowych pracowników.

2) Wyłącznie w sytuacjach wyjątkowych dopuszcza się przetwarzanie danych osobowych w plikach (MS Word, MS Excel) na stacjach roboczych użytkowników, poza bazą danych, znajdująca się w określonym systemie informatycznym. Rejestry zawierające dane osobowe wykonywane w plikach (MS Word, MS Excel) mają tylko charakter tymczasowy i pomocniczy dla dokumentacji papierowej.

3) Przetwarzanie danych na stacji lokalnej lub w innym formacie, np. dane do raportu w postaci pliku arkusza kalkulacyjnego, możliwe jest pod warunkiem, iż zapisane dane będą należycie chronione, tj.

a) uniemożliwi się dostęp do danych osobom nieuprawnionym,

b) uniemożliwi się zmiany danych, a tym samym zafałszowanie informacji pochodzących z systemu,

c) zabezpieczy się bezpośredni dostęp do danych hasłem.

4) Doraźny zbiór danych osobowych należy usunąć z nośnika danych, na którym został utworzony lub zniszczyć nośnik, nie później niż 3 dni po wykorzystaniu danych.

6. Zasady postępowania z komputerami przenośnymi

1) Użytkownik systemu informatycznego, używający komputer przenośny zawierający dane osobowe, zobowiązany jest zachować szczególna ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych.

2) Użytkownik systemu informatycznego używający komputer przenośny zawierający dane osobowe w szczególności powinien:

a)stosować ochronę kryptograficzna;

b) zabezpieczyć dostęp do komputera przenośnego na poziomie systemu operacyjnego - identyfikator i hasło;

c) nie zezwalać na używanie komputera przenośnego osobom nieupoważnionym;

d) zachować szczególna ostrożność przy podłączaniu do sieci publicznych.

3) Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego formalny użytkownik.

7. Zasady korzystania z sieci publicznej (Internet)

1. Użytkownik zobowiązany jest do korzystania z sieci publicznej wyłącznie w celach służbowych
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z sieci publicznej
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem)
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, musi pojawić się odpowiednia ikonka (kłódka) oraz adresu www rozpoczynającego się frazą"https:"

8. Zasady korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione
2. W przypadku przesyłania informacji wrażliwych wewnątrz organizacji bądź wszelkich danych osobowych poza organizację należy wykorzystywać mechanizm haseł lub podpis elektroniczny
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków zawierające: duże i małe litery, cyfry lub znaki specjalne, a hasło należy przesłać odrębnym mailem.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata
6. Nie należy otwierać załączników (plików) oraz nieznanych adresów www (hiperłączy) w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę
7. Użytkownicy nie powinni rozsyłać za pośrednictwem maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia", itp.
8. Użytkownicy nie powinni rozsyłać, maili zawierających załączniki o dużym rozmiarze powyżej 10 MB.
9. Użytkownicy powinni okresowo kasować niepotrzebne maile
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW"

9. Procedura nadawania uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym

Zasady regulujące nadawanie uprawnień do przetwarzania danych oraz rejestrowania uprawnień w systemie informatycznym określono w procedurze **PRO_1 - „Nadawanie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym."**

Procedura obowiązuje wszystkie osoby zaangażowane w proces nadawania uprawnień w systemie informatycznym, a w szczególności kierowników komórek organizacyjnych lub bezpośrednich przełożonych użytkowników systemu informatycznego, Administratora Systemu Informatycznego, a także Administratora Bezpieczeństwa Informacji.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

10. Stosowane metody i środki uwierzytelniania oraz procedury związanych z ich zarządzaniem i użytkowaniem

Zasady dotyczące stosowanych metod i środków uwierzytelniania w systemie informatycznym Urzędu Gminy określono w procedurach:

a) **PRO_2 - „Stosowane metody i środki uwierzytelniania. Ogólne zasady";**
b) **PRO_3 - „Stosowane metody i środki uwierzytelniania. Hasła administracyjne".**

Procedury obowiązują wszystkie osoby mające uprawnienia do przetwarzania danych osobowych w systemie informatycznym, a także Administratora Systemu Informatycznego.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszych procedur.

11. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym

Zasady dotyczące rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym określono w procedurze **PRO_4 - „Rozpoczęcie, zawieszenie i zakończenie pracy w systemie informatycznym".**

Procedura obowiązuje wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemie informatycznym Urzędu Gminy.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

12. Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

Zasady dotyczące tworzenia kopii zapasowych zawierających dane osobowe, a także programów i narzędzi wykorzystywanych do przetwarzania danych określono w procedurze **PRO_5 - „Tworzenie kopii zapasowych zbiorów danych osobowych".**

Procedura obowiązuje Administratora Systemu Informatycznego.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

13. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

Zasady dotyczące sposobu, miejsca i okresu przechowywania zarówno elektronicznych nośników informacji jak i kopii zapasowych zawierających dane osobowe określono w procedurze **PRO_6 - „Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych".**

Procedura obowiązuje wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemie informatycznym przy użyciu elektronicznych nośników informacji, a także Administratora Systemu Informatycznego.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

14. Zabezpieczenie systemu informatycznego przed działalnością nieuprawnionego oprogramowania

Zasady dotyczące stosowania profilaktyki antywirusowej określono w procedurze **PRO_7 - „Zabezpieczenie systemu informatycznego przed działalnością nieuprawnionego oprogramowania".**

Procedura obowiązuje wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemie informatycznym, a także Administratora Systemu Informatycznego.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

15. Odnotowywanie w systemie informatycznym informacji o udostępnianiu danych

Zasady dotyczące odnotowywania informacji w systemie informatycznych, o których mowa w §7 ust. 1 pkt 4 rozp. MSWIA określono w procedurze **PRO_8 - „Odnotowanie w systemie informacji i udostępnianiu danych".**

Procedura obowiązuje wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemie informatycznym.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

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

Zasady dotyczące wykonywania przeglądów i konserwacji systemów informatycznych oraz nośników informacji służących do przetwarzania danych określono w procedurze **PRO_9 - „Wykonywanie przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych".**

Procedura obowiązuje Administratora Systemu Informatycznego.

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za nadzór nad stosowaniem niniejszej procedury.

17. Procedury

PRO_1 - „Nadawanie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym."

PRO_2 - „Stosowane metody i środki uwierzytelniania. Ogólne zasady";

PRO_3 - „Stosowane metody i środki uwierzytelniania. Hasła administracyjne".

PRO_4 - „Rozpoczęcie, zawieszenie i zakończenie pracy w systemie informatycznym".

PRO_5 - „Tworzenie kopii zapasowych zbiorów danych osobowych".

PRO_6 - „Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych".

PRO_7 - „Zabezpieczenie systemu informatycznego przed działalnością nieuprawnionego oprogramowania".

PRO_8 - „Odnotowanie w systemie informacji i udostępnianiu danych".

PRO_9 - „Wykonywanie przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych".

Nadawanie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym

1. Cel procedury

Celem procedury jest określenie zasad zarządzania prawami dostępu dla użytkowników systemu informatycznego oraz administratorów systemu.

2. Zakres obowiązywania

Procedura obowiązuje wszystkie osoby zaangażowane w proces nadawania uprawnień w systemie informatycznym a w szczególności kierowników komórek organizacyjnych lub bezpośrednich przełożonych użytkowników systemu informatycznego, Administratora Systemu Informatycznego a także Administratora Bezpieczeństwa Informacji.

3. Odpowiedzialność

1. Kierownicy komórek organizacyjnych lub bezpośredni przełożeni użytkownika za:
   a) wnioskowanie o przyznanie, zmianę lub cofnięcie uprawnień użytkownikom systemu.
2. Administrator Systemu Informatycznego za:
   a) nadawanie uprawnień zgodnie z wnioskiem;
   b) weryfikację nadanych uprawnień;
   c) nadzór nad zasadnością posiadanych uprawnień.
3. Użytkownicy systemu informatycznego za:
   a) zmianę hasła startowego.
4. Administrator Bezpieczeństwa Informacji za:
   a) nadzór nad zasadnością posiadanych uprawnień.
   b) prowadzenie dokumentacji związanej z nadawaniem uprawnień;
   c) nadzór nad stosowaniem procedury.

4. Opis postępowania

Zarządzanie uprawnieniami użytkownika

1. Przyznanie, zmiana lub cofnięcie uprawnień użytkownikowi do przetwarzania danych osobowych w systemie informatycznym realizowane jest na pisemny wniosek bezpośredniego przełożonego. Wniosek przekazywany jest Administratorowi Bezpieczeństwa Informacji.

2. Użytkownikowi mogą być nadane wyłącznie uprawnienia, które są konieczne do realizacji zleconych mu zadań.

3. Administrator Bezpieczeństwa Informacji zobowiązany jest do sprawdzenia, czy użytkownik, którego wniosek dotyczy:

a) odbył szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych;
b) został upoważniony do przetwarzania danych osobowych;
c) podpisał oświadczenie dotyczące zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, a także dotyczące przetwarzania danych osobowych zgodnie z przepisami prawa.

4. W przypadku braku spełnienia wymagań o których mowa w ust. 3 pkt a-c, Administrator Bezpieczeństwa Informacji wstrzymuje dalszy proces nadawania uprawnień do czasu spełnienia ww. wymagań i informuje o tym fakcie wnioskodawcę.

5. W przypadku spełnienia wymagań o których mowa w ust. 3 pkt a-c, Administrator Bezpieczeństwa Informacji przekazuje wniosek bezpośrednio Administratorowi Systemu Informatycznego w celu nadania identyfikatora oraz wnioskowanych uprawnień w systemie informatycznym.

6. Administrator Systemu Informatycznego nadaje użytkownikowi unikalny w skali systemu identyfikator oraz uprawnienia zgodnie z otrzymanym wnioskiem. Identyfikatory muszą zapewniać jednoznaczną identyfikację.

7. Administrator Systemu Informatycznego po nadaniu wnioskowanych uprawnień oraz identyfikatora, generuje hasło startowe, które następnie przekazuje bezpośrednio użytkownikowi, któremu zostały nadane uprawnienia.

8. Przy pierwszym logowaniu do systemu, użytkownik ma obowiązek zmienić nadane mu hasło.

9. Użytkownik systemu po zalogowaniu zobowiązany jest do sprawdzenia poprawności nadanych mu uprawnień. W przypadku stwierdzenia jakichkolwiek nieprawidłowości związanych z

nadanymi uprawnieniami, użytkownik niezwłocznie informuje o tym fakcie Administratora Bezpieczeństwa Informacji. Administrator Bezpieczeństwa Informacji informuje Administratora Systemu Informatycznego o zgłoszonych nieprawidłowościach, który zobowiązany jest niezwłocznie zablokować dostęp użytkownika do systemu informatycznego i weryfikacji przyznanych uprawnień.

10. Jeżeli nadanie wnioskowanych uprawnień może grozić naruszeniem standardów bezpieczeństwa systemu, Administrator Systemu Informatycznego informuje o tym fakcie Administratora Bezpieczeństwa Informacji i wstrzymuje proces nadawania uprawnień.

11. Administrator Systemu Informatycznego po nadaniu identyfikatora oraz uprawnień w systemie informatycznym, uzupełnia wniosek a następnie przekazuje go Administratorowi Bezpieczeństwa Informacji.

12. Przełożony użytkownika systemu jest zobowiązany do informowania Administratora Bezpieczeństwa Informacji o wszelkich zmianach dotyczących użytkownika, takie jak rozwiązanie umowy o pracę lub cofnięcie upoważnienia do przetwarzania danych osobowych. Zgłoszone zmiany dotyczące użytkownika są przesłanką do niezwłocznego wyrejestrowania użytkownika z systemu informatycznego.

13. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielony innej osobie.

14. Nadanie uprawnień do przetwarzania danych osobowych w systemie informatycznym jak i ich aktualizacja lub cofnięcie następuje każdorazowo na wniosek akceptowany w tym samym trybie.

15. Administrator Bezpieczeństwa Informacji w porozumieniu z Administratorem Systemu Informatycznego ma obowiązek okresowej kontroli i weryfikacji zasadności posiadanych przez użytkowników uprawnień (przynajmniej raz na 3 miesiące). W przypadku niezasadności, dostęp do systemu powinien być niezwłocznie cofnięty.

Zarządzanie uprawnieniami administratorów

1. Konta umożliwiające działania administracyjne (np. root, Administrator) muszą zapewniać pełną rozliczalność i identyfikowalność działań. W tym celu konta z uprawnieniami administracyjnymi powinny być przypisane do konkretnych osób.

2. Administrator Systemu Informatycznego zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie konta umożliwiającego działania administracyjne dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas wprowadzanych zmian w administrowanym systemie.

5. Załączniki

1. **Załącznik_PRO_1_1** – Wniosek o nadanie uprawnień
2. **Załącznik_PRO_1_2** – Imienna ewidencja uprawnień

Stosowane metody i środki uwierzytelniania. Ogólne zasady.

1. Cel procedury

Celem procedury jest określenie ogólnych zasad związanych z zarządzaniem identyfikatorami oraz hasłami użytkowników systemu informatycznego.

2. Zakres obowiązywania

Procedura obowiązuje wszystkie osoby mające uprawnienia do przetwarzania danych osobowych w systemie informatycznym.

3. Odpowiedzialność

1. Administrator Systemu Informatycznego za:

   a) nadzór nad stosowanymi metodami i środkami uwierzytelniania w systemie informatycznym;
   b) nadawanie identyfikatorów oraz haseł zgodnie z zasadami określonymi w procedurze.

2. Użytkownicy systemu informatycznego za:

   a) stosowanie się do zasad określonych w niniejszej procedurze.

3. Administrator Bezpieczeństwa Informacji za:

   a) nadzór nad stosowaniem procedury.

4. Opis postępowania

1. Wymagania dotyczące identyfikatorów:

   a) znaki w identyfikatorze nie mogą być rozdzielone spacjami oraz zawierać polskich znaków;
   b) identyfikator jest unikalny w skali całego systemu;
   c) identyfikator jest przypisany tylko do jednej osoby i tylko ona może nim się posługiwać;
   d) niedopuszczalne jest zmienianie identyfikatora użytkownika.

2. Wymagania dotyczące haseł:

   a) hasło musi zawierać nie mniej niż 8 znaków;
   b) hasło musi składać się z liter (małych i dużych) oraz cyfr lub znaków specjalnych;
   c) hasło musi być zmieniane przez użytkownika nie rzadziej niż raz na 30 dni;
   d) hasło nie może zawierać polskich znaków;

e) hasła nie mogą być powszechnie używanymi słowami;
f) hasła powinny być trudne do odgadnięcia a w szczególności nie powinny zawierać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów lub innych informacji bezpośrednio kojarzących się z użytkownikiem;
g) niedopuszczalne jest, aby hasło było takie same jak identyfikator;
h) hasła do różnych systemów informatycznych powinny być różne, za wyjątkiem sytuacji gdy jest możliwe zastosowanie mechanizmu jednokrotnego logowania;
i) hasła nie mogą być ujawniane innym użytkownikom;
j) 3-krotna błędna próba wprowadzenia hasła (o ile jest to możliwe) powinna skutkować zablokowaniem konta użytkownika oraz odpowiednią adnotacją w systemie monitoringu zawierającą minimum: identyfikator urządzenia komputerowego, na którym próbowano dokonać logowania oraz czas wykrycia zdarzenia;
k) tworzona jest historia haseł (o ile jest to możliwe), przynajmniej 12 wstecz, w celu zablokowania ich powtarzania. Jeżeli system nie umożliwia tworzenia historii haseł należy unikać ponownego lub cyklicznego używania starych haseł;
l) hasła nie mogą być przechowywane w czytelnej postaci, zarówno jako tekst w pliku jak i zapisane na papierze. Wyjątkiem jest zdeponowanie haseł użytkowników lub administratorów systemu w bezpiecznym miejscu (np. sejf, szafa pancerna), w zamkniętej kopercie opisanej nazwiskiem osoby upoważnionej do jej otwarcia;
m) hasła tymczasowe lub startowe należy zmienić zaraz po pierwszym logowaniu.

3. Pozostałe wymagania dotyczące metod i środków uwierzytelniania w systemie informatycznym:

a) dostęp do danych osobowych w systemie informatycznym realizowany jest po podaniu unikalnego w skali systemu identyfikatora użytkownika oraz prawidłowego hasła;
b) użytkownicy systemu informatycznego są odpowiedzialni za wszelkie działania prowadzone w systemie informatycznym z użyciem ich identyfikatora oraz hasła;
c) zabrania się, aby użytkownik systemu informatycznego korzystał z kont: administrator, gość, a także z konta innego użytkownika systemu;
d) użytkownik ma obowiązek stosować zasady bezpieczeństwa podczas logowania, jak i procesu aktualizacji haseł uniemożliwiające kompromitację jego hasła;
e) w przypadku, gdy użytkownik ma podejrzenia co do skompromitowania jego hasła, zobowiązany jest do niezwłocznej zmiany hasła i poinformowania o tym fakcie Administratora Bezpieczeństwa Informacji;
f) udostępnienie hasła postronnej osobie należy traktować jako poważny incydent naruszenia ochrony danych osobowych.

5. Załączniki

Brak.

WÓJT
mgr Tomasz Lato

Stosowane metody i środki uwierzytelniania. Hasła administracyjne.

1. Cel procedury

Celem procedury jest określenie zasad związanych z zarządzaniem hasłami administracyjnymi.

2. Zakres obowiązywania

Procedura obowiązuje Administratora Systemu Informatycznego.

3. Odpowiedzialność

1. Administrator Systemu Informatycznego za:

   a) stosowanie się do zasad określonych w niniejszej procedurze.

2. Administrator Bezpieczeństwa Informacji za:

   a) nadzór nad stosowaniem procedury.

4. Opis postępowania

1. Hasła administracyjne ustala Administrator Systemu Informatycznego.

2. Administrator Systemu Informatycznego jest zobowiązany do prowadzenia metryk haseł administratora i przechowywania ich w zamkniętych kopertach, odrębnych dla każdego systemu/aplikacji, w sejfie lub w szafie pancernej, do których dostęp ma wyłącznie Administrator Systemu Informatycznego, Administrator Danych Osobowych oraz Administrator Bezpieczeństwa Informacji;

3. Hasła administracyjne mogą być wykorzystywane wyłącznie w uzasadnionych przypadkach;

4. W przypadku utraty uprawnień przez osobę administrującą danym systemem/aplikacją, należy niezwłocznie zmienić hasła, do których miał dostęp;

5. Administrator Systemu Informatycznego może zmieniać hasła do poszczególnych systemów/aplikacji nie rzadziej niż co 2 miesiące, pod warunkiem iż hasła te składają się z co najmniej 12 znaków;

6. Pozostałe wymagania dotyczące haseł administracyjnych są analogiczne, jak w przypadku haseł użytkowników.

5. Załączniki

1. **Załącznik_PRO_3_1** – Metryka hasła administracyjnego.

6. Dokumenty powiązane

1. **Procedura PRO_2** – Stosowane metody i środki uwierzytelniania. Ogólne zasady.

Rozpoczynanie, zawieszanie i zakończanie pracy w systemie informatycznym.

1. Cel procedury

Celem procedury jest określenie zasad postępowania w przypadku rozpoczynania, zwieszania oraz zakończenia pracy w systemie informatycznym.

2. Zakres obowiązywania

Procedura obowiązuje we wszystkich komórkach organizacyjnych Urzędu Gminy.

3. Odpowiedzialność

1. Administrator Systemu Informatycznego za:
   a) odpowiednią konfigurację wygaszaczy ekranu.
2. Użytkownicy systemu informatycznego za:
   a) przestrzeganie zasad niniejszej procedury.
3. Administrator Bezpieczeństwa Informacji za:
   a) nadzór nad stosowaniem procedury.

4. Opis postępowania

Zasady rozpoczęcia pracy w systemie informatycznym

1. Przed przystąpieniem do pracy, użytkownik zobowiązany jest do sprawdzenia czy stacja robocza wykorzystywana do przetwarzania danych osobowych w systemie informatycznym nie wskazuje na ingerencję osób trzecich, a także czy stanowisko pracy zastano w takim stanie jak pozostawiono po zakończeniu pracy. W przypadku stwierdzenia wszelkich nieprawidłowości, należy niezwłocznie o tym fakcie powiadomić Administratora Bezpieczeństwa Informacji.

2. Przed uruchomieniem stacji roboczej, użytkownik zobowiązany jest do upewnienia się, czy ekran monitora jest ustawiony w sposób uniemożliwiający osobom nieupoważnionym podglądnięcie jego zawartości.

3. Użytkownik zobowiązany jest zwrócić uwagę, czy w trakcie uruchamiania stacji roboczej pojawiają się komunikaty systemowe sugerujące problemy z działaniem komputera, ingerencję osób nieupoważnionych itp. W przypadku stwierdzenia wszelkich nieprawidłowości, należy niezwłocznie o tym fakcie powiadomić Administratora Bezpieczeństwa Informacji.

4. Pracę w systemie informatycznym użytkownik rozpoczyna po uwierzytelnieniu się w systemie za pomocą własnego identyfikatora oraz hasła.

5. W trakcie pracy, użytkownik powinien mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych.

6. W trakcie pracy, użytkownik powinien mieć na biurku tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych.

Zasady zawieszenia pracy w systemie informatycznym

1. Podczas przerwy w pracy, zarówno zaplanowanej jak i niezaplanowanej, pracownik zobowiązany jest do zabezpieczenia stanowiska pracy jak również sprzętu komputerowego przed dostępem osób nieupoważnionych, a w szczególności do:

a) do wylogowania się z systemu bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji przez osoby niepowołane poprzez wciśnięcie klawiszy „Windows+L" lub „CTRL+ALT+DEL" i wybranie opcji „Zablokuj stację roboczą";
b) zabezpieczenia wszelkich dokumentów i nośników zawierających dane osobowe przed dostępem osób nieupoważnionych.

2. W przypadku bezczynności użytkownika na stacji roboczej trwającej więcej niż 10 min, uruchamiany jest automatycznie wygaszacz ekranu. Wznowienie pracy możliwe jest po ponownym uwierzytelnieniu się poprzez podanie własnego identyfikatora oraz hasła.

3. Opuszczając pomieszczenie użytkownik zobowiązany jest do zamknięcia drzwi na klucz, za wyjątkiem, gdy w pomieszczeniu pozostała inna upoważniona osoba.

Zasady zakończenia pracy w systemie informatycznym

1. Użytkownik kończąc pracę, zobowiązany jest do wylogowania się ze wszystkich używanych aplikacji i ich zamknięcia oraz do wyłączenia stacji roboczej.

2. Użytkownik zobowiązany jest do zabezpieczenia wszystkich dokumentów i nośników zawierających dane osobowe, w celu uniemożliwienia dostępu do nich osób nieupoważnionych.

3. Użytkownik zobowiązany jest sprawdzić czy:

a) wszystkie urządzenia elektryczne zostały wyłączone;
b) w urządzeniach typu drukarka, fax, ksero nie zostały pozostawione wydruki zawierające dane osobowe;
c) szafy i szafki zostały pozamykane na klucz;
d) klucze do szaf i szafek zostały schowane;
e) zamknięte zostały wszystkie okna.

4. Opuszczając pomieszczenie użytkownik zobowiązany jest do zamknięcia drzwi na klucz, za wyjątkiem, gdy w pomieszczeniu pozostała inna upoważniona osoba.

5. Załączniki

Brak.

Tworzenie kopii zapasowych zbiorów danych osobowych.

1. Cel procedury

Celem procedury jest określenie zasad związanych z tworzeniem kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania..

2. Zakres obowiązywania

Procedura obowiązuje Administratora Systemu Informatycznego.

3. Odpowiedzialność

1. Administrator Systemu Informatycznego za:

   a) wykonywanie kopii zapasowych oraz weryfikację poprawności ich wykonania.

2. Administrator Bezpieczeństwa Informacji za:

   a) nadzór nad stosowaniem procedury.

4. Opis postępowania

1. Kopie zapasowe tworzone są w sposób, zapewniający odtworzenie wszystkich informacji w przypadku awarii.

2. Kopie zapasowe oprogramowania systemowego oraz plików konfiguracyjnych wykonywane są po każdej zmianie administracyjnej w systemie.

3. Kopie zapasowe wykonywane są automatycznie na przeznaczonej do tego celu macierzy dyskowej.

4. Jeżeli macierz dyskowa przeznaczona do wykonywania kopii zapasowych znajduje się w tym samym pomieszczeniu, co serwery odpowiedzialne za pracę systemów informatycznych, w takim wypadku Administrator Systemu Informatycznego jest zobowiązany do zapewnienia redundancji kopii zapasowych i przechowywania dodatkowego zestawu kopii zapasowych w innym, wyznaczonym do tego celu pomieszczeniu (lub budynku, o ile to możliwe). Kopie te należy

przechowywać w sejfie lub szafie pancernej do której dostęp ma tylko Administrator Bezpieczeństwa Informacji oraz Administrator Systemu Informatycznego.

5. Kopią zapasową objęte są:

a) bazy danych zawierających zbiory danych osobowych;
b) programy i narzędzia programowe służące do przetwarzania danych;
c) dane konfiguracyjne systemu informatycznego;
d) logi systemowe;
e) pozostałe zasoby zawierające dane osobowe.

6. W celu zapewnienia bezpieczeństwa pracy systemu informatycznego oraz możliwości odtworzenia danych po wystąpieniu awarii stosuje się następujący harmonogram tworzenia kopii zapasowych:

a) codzienne wykonywana jest kopia zapasowa przyrostowa;
b) co tydzień wykonywana jest kopia zapasowa pełna.

7. W celu zweryfikowania poprawności danych przechowywanych na kopiach zapasowych oraz możliwości przywrócenia ich do stanu sprzed awarii, Administrator Systemu Informatycznego wykonuje okresowe testy kopii zapasowych. W przypadku danych o szczególnym znaczeniu weryfikacja wykonywana jest nie rzadziej niż raz na 14 dni.

8. Kopia pełna wraz z następującymi po niej kopiami przyrostowymi stanowią zestaw pozwalający na odtworzenie danych do chwili wykonania ostatniej kopii przyrostowej.

9. Administrator Systemu Informatycznego jest zobowiązany do przechowywania co najmniej 5 zestawów kopii zapasowych, zapisanych jeden po drugim.

10. Zestaw kopii zapasowych może zostać użyty w przypadku wystąpieniu awarii po okresie nie krótszym niż 4 tygodnie.

11. Kopie wykonywane na nośnikach zewnętrznych, np. CD/DVD, streamer, HDD itp. należy opisywać. Opis powinien zawierać co najmniej:

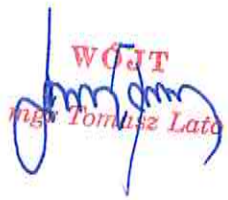
a) oznaczenie nośnika;
b) numer kolejny nośnika;
c) data wykonania kopii;
d) typ kopii;

e) nazwa systemu informatycznego, zbiory danych osobowych lub inne informacje jednoznacznie opisujące zawartość kopii zapasowej;
f) identyfikator osoby, która wykonała kopię

12. Nośniki kopii zapasowych, które zostały wycofane z użycia, należy pozbawić zapisanych danych w sposób uniemożliwiający ich odczytanie przez osoby nieuprawnione. Jeżeli usunięcie danych jest niemożliwe, należy zniszczyć fizycznie nośnik w sposób adekwatny do rodzaju nośnika.

5. Załączniki

Brak.



Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych.

1. Cel procedury

Celem procedury jest określenie zasad dotyczących sposobów, miejsca i okresu przechowywania elektronicznych nośników informacji a także kopii zapasowych zawierających dane osobowe.

2. Zakres obowiązywania

Procedura obowiązuje we wszystkich komórkach organizacyjnych Urzędu Gminy.

3. Odpowiedzialność

1. Użytkownicy systemu informatycznego za

   a) stosowanie się do zasad określonych w procedurze.

2. Administrator Systemu Informatycznego za:

   a) zarządzanie elektronicznymi nośnikami informacji zawierającymi dane osobowe.

3. Administrator Bezpieczeństwa Informacji za:

   a) nadzór nad stosowaniem procedury.

4. Opis postępowania

1. Zabronione jest korzystanie z prywatnych lub niezewidencjonowanych elektronicznych nośników informacji.

2. Dane osobowe mogą zostać zapisane na przenośnych elektronicznych nośnikach informacji w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub niebezpieczne.

3. Elektroniczne nośniki informacji należy przechowywać w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.

4. Elektroniczne nośniki informacji należy zabezpieczać przed zagrożeniami środowiskowymi (zalanie, pożar itp.).

5. Elektroniczne nośniki informacji należy zabezpieczyć przed nieuprawnionym dostępem poprzez stosowanie kryptograficznych środków ochrony.

6. Każdy elektroniczny nośnik informacji przydzielony pracownikowi może być wykorzystywany wyłącznie do celów służbowych.

7. Dane przechowywane na elektronicznych nośnikach informacji są własnością Urzędu Gminy.

8. Zabronione jest wynoszenie poza obszar Urzędu Gminy wymiennych nośników informacji zawierających dane osobowe bez zgody Administratora Danych Osobowych.

9. W przypadku przekazywania elektronicznych nośników informacji poza obszar Urzędu Gminy należy stosować następujące zasady bezpieczeństwa:

a) adresat powinien zostać powiadomiony o przesyłce;
b) nadawca powinien sporządzić kopię przesyłanych danych;
c) dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą;
d) stosować bezpieczne koperty depozytowe;
e) adresat powinien powiadomić nadawcę o otrzymaniu przesyłki.

10. Elektroniczne nośniki informacji wykorzystywane są i przechowywane do czasu ustania ich użyteczności po czym należy trwale pozbawić je danych.

11. Nośniki, których z różnych przyczyn nie można pozbawić zapisu, należy uszkodzić w sposób uniemożliwiający ich odczytanie.

12. Nośniki z kopiami zapasowymi są przechowywane przez Administratora Systemu Informatycznego w wyznaczonym do tego celu miejscu, w szafie zamykanej na klucz. Dostęp do szafy ma wyłącznie Administrator Bezpieczeństwa Informacji oraz Administrator Systemu Informatycznego.

13. Administrator Systemu Informatycznego jest zobowiązany do przechowywania co najmniej 5 zestawów kopii zapasowych, zapisanych jeden po drugim. Po ustaniu użyteczności, nośniki z kopiami są trwale niszczone

5. Załączniki

1. **Załącznik_PRO_6_1** – Rejestr nośników zawierających dane osobowe.

WÓJT
mgr Tomasz Lato

Zabezpieczenie systemu informatycznego przed działalnością nieuprawnionego oprogramowania.

1. Cel procedury

Celem procedury jest określenie zasad zabezpieczenia systemu informatycznego przed działalnością nieuprawnionego oprogramowania.

2. Zakres obowiązywania

Procedura obowiązuje we wszystkich komórkach organizacyjnych Urzędu Gminy Masłów, gdzie użytkownicy systemu informatycznego przetwarzają dane osobowe przy wykorzystaniu komputerów.

3. Odpowiedzialność

1. Użytkownicy systemu informatycznego za:

   a) profilaktykę antywirusową na swoich stanowiskach komputerowych.

2. Administrator Systemu Informatycznego za:

   a) wdrożenie i prawidłowe działanie oprogramowania antywirusowego oraz zapór ogniowych;
   b) bieżącą kontrolę antywirusową;
   c) obsługę zgłoszeń w sytuacji naruszenia ochrony antywirusowej.

3. Administrator Danych Osobowych za:

   a) zapewnienie odpowiedniego oprogramowania antywirusowego.

4. Administrator Bezpieczeństwa Informacji za:

   a) nadzór nad stosowaniem procedury.

4. Opis postępowania

1. Każda stacja robocza oraz serwer wyposażone są w monitor antywirusowy.

2. Monitor antywirusowy jest uruchamiany automatycznie podczas uruchomienia systemu operacyjnego.

3. Oprogramowanie antywirusowe zapewnia ochronę: systemu operacyjnego, przechowywanych plików, poczty wychodzącej i przychodzącej.

4. Oprogramowanie antywirusowe powinno być skonfigurowane w sposób wymuszający automatyczne usuwanie wirusów, zaś w przypadku, gdy ich usunięcie jest niemożliwe, obejmowanie ich kwarantanną.

5. Dokonywanie zmian w konfiguracji oprogramowania antywirusowego jest możliwa tylko przez Administratora Systemu Informatycznego.

6. Użytkownik systemu zobowiązany jest do bieżącego sprawdzania programem antywirusowym:

a) wszystkich plików na nośnikach elektronicznych;
b) plików otrzymywanych przez sieć;
c) załączników poczty elektronicznej.

7. Użytkownik zobowiązany jest poinformować niezwłocznie Administratora Systemu Informatycznego o zauważonych nieprawidłowościach działania stacji roboczej, mogących wskazywać na zainfekowanie wirusem.

8. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, należy o takim przypadku niezwłocznie poinformować Administratora Systemu Informatycznego. Przypadek taki stanowi incydent bezpieczeństwa. Obowiązkiem ASI jest podjąć działania zmierzające do usunięcia zagrożenia tj.: usunięcia zainfekowanych plików oraz o ile jest taka potrzeba, odtworzenia usuniętych plików z kopii zapasowych.

9. Administrator Systemu Informatycznego prowadzi rejestr wszystkich przypadków wykrycia wirusów, w którym odnotowywane są następujące informacje:

a) oznaczenie komputera na którym został wykryty wirus;
b) czas wykrycia;
c) rodzaj wirusa;
d) podjęta akcja naprawcza;
e) uwagi dodatkowe.

10. Każdy serwer oraz stacja robocza pracują z włączoną zaporą ogniową (firewall).

11. Sieć lokalna urzędu zabezpieczona jest na styku z siecią publiczną urządzeniem sprzętowym (firewall) z uruchomionym systemem IPS do wykrywania i blokowania ataków do sieci lokalnej. Zastosowano mechanizmy monitorujące przeglądanie sieci publicznej przez użytkowników.

Uwzględniają one:
Blokowanie stron internetowych niebezpiecznego typu (np.: kategoria sex, hazard itp.)
Analizę przesyłanych informacji pod kątem niebezpiecznego oprogramowania
Analizę odwiedzania stron internetowych
Analizę poczty

5. Załączniki

Brak.

WÓJT
mgr Tomasz Lato

Realizacja wymogów, o których mowa w §7 ust. 1 pkt 4 rozp. MSWIA.

1. Cel procedury

Celem procedury jest określenie zasad związanych ze sposobem odnotowywania informacji w systemie informatycznym dotyczących udostępniania danych osobowych.

2. Zakres obowiązywania

Procedura obowiązuje we wszystkich komórkach organizacyjnych Urzędu Miasta i Gminy.

3. Odpowiedzialność

1. Użytkownicy systemu informatycznego za

   a) profilaktykę antywirusową na swoich stanowiskach komputerowych.

2. Administrator Bezpieczeństwa Informacji za:

   a) nadzór nad stosowaniem procedury.

4. Opis postępowania

1. Dane osobowe udostępnia się osobom lub podmiotom uprawnionym do ich otrzymywania na mocy przepisów prawa.

2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej.

3. W przypadku, gdy udostępniane są dane osobowe znajdujące się w zbiorach danych przetwarzanych w systemie informatycznym, system ten powinien umożliwić odnotowanie następujących informacji:

   a) data udostępnienie;
   b) osoba lub podmiot, której udostępnia się dane;
   c) zakres udostępnionych informacji.

4. W przypadku, gdy w systemie informatycznym służącym do przetwarzania danych osobowych nie jest możliwe odnotowywanie takich informacji, administrator danych odnotowuje je w rejestrze odbiorców danych osobowych. W rejestrze odnotowywane są imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia.

5. Pracownik, który w systemie informatycznym przetwarza dane osobowe jest obowiązany do przekazania administratorowi danych i ABI informacji o odbiorcach, którym dane zostały udostępnione

5. Załączniki

Brak.

WÓJT
mgr Tomasz Lato

Wykonywanie przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych.

1. Cel procedury

Celem procedury jest określenie zasad związanych z wykonywaniem przeglądów i konserwacji systemów informatycznych, a także elektronicznych nośników informacji wykorzystywanych do przetwarzania danych osobowych.

2. Zakres obowiązywania

Procedura obowiązuje Administratora Systemu Informatycznego.

3. Odpowiedzialność

1. Administrator Systemu Informatycznego za:

   a) przeprowadzanie przeglądów i konserwacji oraz ich prawidłowy przebieg;
   b) nadzór nad likwidacją, przekazaniem oraz naprawą nośników informacji;
   c) prowadzenie dokumentacji systemowej.

2. Administrator Bezpieczeństwa Informacji za:

   a) nadzór nad stosowaniem procedury.

4. Opis postępowania

1. Administrator Systemu Informatycznego wykonuje przeglądy i konserwacje systemu informatycznego zgodnie z terminami określonymi przez producentów sprzętu lub oprogramowania lub zgodnie z harmonogramem określonym przez Administratora Systemu Informatycznego, ale nie rzadziej, niż raz w roku.

2. Administrator Systemu Informatycznego odpowiedzialny jest za identyfikację i przyjmowanie zgłoszeń dotyczących nieprawidłowości w działaniu systemu informatycznego w celu niezwłocznego ich usunięcia.

3. Wszelkie prace serwisowe i konserwacyjne systemu informatycznego wykonywane przez podmiot zewnętrzny mogą odbywać się na zasadach określonych w umowie z uwzględnieniem klauzuli dotyczącej ochrony danych osobowych.

4. Wszelkie prace serwisowe i konserwacyjne systemu informatycznego wykonywane doraźnie przez osoby nieposiadające upoważnienia do przetwarzania danych osobowych mogą być wykonywane wyłącznie w obecności Administratora Systemu Informatycznego lub innych osób upoważnionych przez Administratora Danych Osobowych.

5. Przed rozpoczęciem prac serwisowych lub konserwacji systemu informatycznego przez osoby spoza Urzędu Gminy, konieczne jest potwierdzenie tożsamości serwisantów przez Administratora Systemu Informatycznego.

6. Rozpoczęcie prac serwisowych lub konserwacyjnych systemu informatycznego przez osoby spoza Urzędu Gminy poprzedzone jest wcześniejszą informacją o zakresie planowanych prac. Prace mogą zostać rozpoczęte nie wcześniej niż po akceptacji przedstawionego zakresu prac przez Administratora Systemu Informatycznego. Planowany zakres prac Administrator Systemu Informatycznego dołącza do prowadzonej dokumentacji systemowej.

7. Wykonanie prac serwisowych lub konserwacyjnych powinno być potwierdzone raportem wydanym przez osobę serwisującą, opisującym m.in. zakres wykonanych prac. Raport dołączany jest przez Administratora Systemu Informatycznego do prowadzonej dokumentacji systemowej.

8. Administrator Systemu Informatycznego prowadzi dziennik, w którym odnotowywane są wszystkie zdarzenia mające miejsce w systemie informatycznym, a mające wpływ na bezpieczeństwo jego działania.

9. Administrator Systemu Informatycznego jest zobowiązany do prowadzenia dokumentacji dotyczącej przeprowadzanych przeglądów i konserwacji systemu informatycznego. Dokumentacja ta powinna zawierać w szczególności:

a) czas i datę rozpoczęcia przeglądu lub konserwacji;
b) zakres wykonanych prac;
c) wykaz osób przeprowadzających przegląd lub konserwację;
d) czas i datę zakończenia przeglądu lub konserwacji.

10. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane, w tym dane osobowe, przeznaczone do:

a) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
c) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem Administratora Systemu Informatycznego lub innych osób upoważnionych przez Administratora Danych Osobowych.

5. Załączniki

Brak.

WÓJT
mgr Tomasz Lato

WÓJT

mgr Tomasz Lato

URZĄD GMINY MASŁÓW
ul. Spokojna 2, 26-001 Masłów
REG.000547313, NIP 657 17 48 114

Wniosek nr ....

Nadanie uprawnień	Modyfikacja uprawnień	Odebranie uprawnień
☐	☐	☐

Imię i Nazwisko użytkownika:	Stanowisko:
Miejsce przetwarzania danych:	**Dział:**
Identyfikator:	-
	-

Opis zakresu uprawnień:

ADM – uprawnienia administracyjne **P** – przeglądanie **PRN** – drukowanie **A** - archiwizowanie	**D** - dodawanie **E** – edytowanie **U** – usuwanie

Nazwa programu/modułu	ADM	P	PRN	A	D	E	U
1	2	3	4	5	6	7	8

Uwagi:

Data i podpis przełożonego użytkownika SI	

Data i podpis ASI	Data i podpis ABI

WÓJT
mgr Tomasz Lato

URZĄD GMINY MASŁÓW
ul. Spokojna 2, 26-001 Masłów
REG.000547313, NIP 657 17 48 114

Imienna ewidencja uprawnień

L.p.	Imię i Nazwisko osoby uprawnionej	Data	Zakres uprawnień	Identyfikator użytkownika

WÓJT
mgr Tomasz Lato

URZĄD GMINY MASŁÓW
ul. Spokojna 7, 26-401 Masłów
REGON 0005[illegible]7314, NIP 657 17 48 114

Metryka hasła administracyjnego

Opis systemu lub aplikacji, której dotyczy hasło:

.....

.....

.....

.....

.....

HASŁO:

WÓJT
mgr Tomasz Lato

Rejestr nośników zawierających dane osobowe.

Lp.	*Oznaczenie/opis nośnika*	*Opis zawartości nośnika*	*Miejsce przechowywania*	*Uwagi*	*Data wpisu*	*Osoba odpowiedzialna za nośnik*

WÓJT
mgr Tomasz Lato