WÓJT GMINY
MAŁA WIEŚ

Zarządzenie Nr 219/89/2016
Wójta Gminy Mała Wieś
z dnia 17 listopada 2016 roku

w sprawie Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Mała Wieś

Na podstawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U. z 2016 roku poz. 922 z) oraz § 3, 4 i 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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 roku Nr 100, poz. 1024), zarządza się co następuje:

§ 1

1. Ustala się Politykę Bezpieczeństwa w Urzędzie Gminy Mała Wieś stanowiącą załącznik Nr 1 do niniejszego zarządzenia.
2. Wprowadza się Instrukcję Zarządzania Systemem Informatycznym w Urzędzie Gminy Mała Wieś stanowiącą załącznik Nr 2 do niniejszego zarządzenia.

§ 2

Zobowiązuje się:

1. Administratora Bezpieczeństwa Informacji do:
   1) wdrożenia Polityki Bezpieczeństwa w Urzędzie Gminy Mała Wieś, w tym zapoznania z nią użytkowników informacji oraz innych osób zobowiązanych do ochrony i zabezpieczenia danych,
   2) wdrożenia Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Gminy Mała Wieś, w tym zapoznania z nią użytkowników informacji,
   3) przygotowania wymaganych dokumentów związanych z dopuszczeniem i upoważnieniem użytkowników informacji do przetwarzania danych osobowych oraz dostępem osób do obszarów i pomieszczeń przetwarzania danych.
2. Administratora Systemu Informatycznego do wdrożenia zasad i procedur funkcjonowania systemu informatycznego.
3. Użytkowników informacji do:
   1) szczegółowego zapoznania się z Polityką Bezpieczeństwa oraz Instrukcją Zarządzania Systemem Informatycznym w Urzędzie Gminy Mała Wieś,
   2) podpisania przedstawionych przez Administratora Bezpieczeństwa Informacji dokumentów,
   3) podpisania przedstawionych przez Administratora Systemu Informatycznego dokumentów,

4) przestrzegania zasad i procedur ochrony danych osobowych i ich przetwarzania w systemach przetwarzania.

4. Osoby zobowiązane do ochrony i zabezpieczenia danych do:
   1) szczegółowego zapoznania się z Polityką Bezpieczeństwa w Urzędzie Gminy Mała Wieś,
   2) podpisania przedstawionych przez Administratora Bezpieczeństwa Informacji dokumentów,
   3) przestrzegania zasad i procedur zabezpieczenia danych.

§ 3

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji oraz Administratorowi Systemu Informatycznego.

§ 4

Traci moc Zarządzenie Nr 202/39/2013 Wójta Gminy Mała Wieś z dnia 2 lipca 2013 roku w sprawie Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Gminy Mała Wieś.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Zygmunt Wojnarowski

URZĄD GMINY
MAŁA WIEŚ

Załącznik Nr 2
do Zarządzenia nr 219/89/2016
Wójta Gminy Mała Wieś
z dnia 17 listopada 2016 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

SPIS TREŚCI

I. Cel

Instrukcja określa sposób zarządzania systemem informatycznym, wykorzystywanym do przetwarzania danych osobowych przez Administratora Danych – w celu zabezpieczenia ich przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, uszkodzeniem, zniszczeniem lub utratą.

II. Definicje

Ilekroć jest mowa o:

1) ***ustawie*** – należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922),
2) ***rozporządzeniu*** - należy przez to rozumieć rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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),
3) ***Administratorze Danych*** - należy przez to rozumieć Wójta Gminy Mała Wieś,
4) ***Administratorze Bezpieczeństwa Informacji*** – należy przez to rozumieć Podinspektora ds. zarządzania kryzysowego, obrony cywilnej i spraw obronnych, ochrony informacji niejawnych i ochrony danych osobowych pisemnie upoważnionego przez **Administratora Danych** do nadzorowania przestrzegania zasad przetwarzania danych i informacji oraz wymagań w zakresie ich ochrony, określonych w Polityce Bezpieczeństwa oraz wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych,
5) ***Administratorze Systemu Informatycznego*** – należy przez to rozumieć pracownika Urzędu Gminy Mała Wieś pisemnie wyznaczonego przez **Administratora Danych**, nadzorującego funkcjonowanie systemu informatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony użytkowanych w tym systemie,
6) ***Administratorach Informacji*** – należy przez to rozumieć Zastępcę Wójta - Sekretarza Gminy i Skarbnika Gminy oraz inne osoby decydujące o narzędziach, metodach, miejscu i czasie przetwarzania, przechowywania, tworzenia i niszczenia informacji chronionych w komórkach organizacyjnych,
7) ***Użytkownikach Informacji*** – należy przez to rozumieć upoważnionych na piśmie pracowników Urzędu Gminy Mała Wieś, którym nadano identyfikator i przyznano hasło, mających dostęp do informacji chronionych. Użytkownikiem informacji może być również osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż, wolontariusz lub inna osoba pod warunkiem uzyskania upoważnienia,
8) ***Informacji chronionej*** – należy przez to rozumieć wszelkie zapisy na papierze, w układach elektronicznych, na nośnikach magnetycznych, optycznych itp., które ze względu na dobro Urzędu Gminy Mała Wieś lub jego interesantów podlegają ochronie przed nieautoryzowanym dostępem, powieleniem, ujawnieniem, modyfikacją, wykorzystaniem, zniszczeniem, utratą, kradzieżą lub zatajeniem,
9) ***Przetwarzaniu*** – należy przez to rozumieć dokonywanie jakichkolwiek operacji na danych i informacjach, w szczególności, takich jak zbieranie, przechowywanie, opracowywanie, zmienianie, kopiowanie, udostępnianie i usuwanie, a zwłaszcza tych, które wykonuje się w systemach informatycznych,
10) ***Systemach przetwarzania*** – należy przez to rozumieć systemy tradycyjne oraz systemy informatyczne, w których dokonywane są operacje na danych i informacjach,
11) ***Systemie tradycyjnym*** – należy przez to rozumieć wszelką dokumentację papierową zawierającą informacje o funkcjonowaniu Urzędu Gminy Mała Wieś lub jego

interesantach – kartoteki, skorowidze, księgi, wykazy, rejestry, ewidencje i inne zbiory danych i informacji, w tym korespondencję z interesantami Urzędu Gminy Mała Wieś,

12) ***Systemie informatycznym*** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania oraz narzędzi programowych zastosowanych w celu przetwarzania danych i informacji,
13) ***Sieci lokalnej*** – należy przez to rozumieć połączenie poszczególnych urządzeń systemu informatycznego Urzędu Gminy Mała Wieś wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci Internet,
14) ***Teletransmisji*** – należy przez to rozumieć przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
15) ***Identyfikatorze*** - należy przez to rozumieć ciąg znaków literowych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych w systemie informatycznym,
16) ***Haśle*** - należy przez to rozumieć ciąg znaków literowych, cyfrowych lub znaków specjalnych znanych jedynie osobie uprawnionej do pracy w systemie informatycznym,
17) ***Uwierzytelnianiu*** - należy przez to rozumieć działanie, którego celem jest weryfikacja deklarowanej tożsamości użytkownika informacji,
18) ***Rozliczalności*** - należy przez to rozumieć właściwość zapewniającą, że działania mogą być przypisane w sposób jednoznaczny tylko Urzędowi Gminy Mała Wieś,
19) ***Integralności danych*** - należy przez to rozumieć właściwość zapewniającą, że dane i informacje nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
20) ***Poufności danych*** - należy przez to rozumieć właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

III. Poziom bezpieczeństwa

Uwzględniając kategorie danych osobowych, prawidłową ochronę i zapewnienie bezpieczeństwa ich przetwarzania oraz fakt połączenia systemu informatycznego z siecią publiczną, w Urzędzie Gminy Mała Wieś wprowadza się wysoki poziom bezpieczeństwa, w rozumieniu § 6 rozporządzenia.

IV. Procedury nadawania i zmiany uprawnień do przetwarzania danych oraz ich rejestrowania w systemach informatycznych

Każdy użytkownik systemu informatycznego przed przystąpieniem do przetwarzania danych i informacji musi zapoznać się z:

1) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016r., poz. 922), jeżeli wykonywane obowiązki służbowe są związane z danymi osobowymi,
2) Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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),
3) Zarządzeniem Nr 218/88/2016 Wójta Gminy Mała Wieś z dnia 17 listopada 2016 roku w sprawie wykonywania ustawy o ochronie danych osobowych w Urzędzie Gminy Mała Wieś,
4) Zarządzeniem Nr 219/89/2016 Wójta Gminy Mała Wieś z dnia 17 listopada 2016 roku w sprawie Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Mała Wieś,
5) Podstawowymi zagrożeniami związanymi z przetwarzaniem danych oraz zastosowanymi środkami technicznymi i organizacyjnymi w celu ich ochrony.

1. Podstawowe zasady nadawania i rejestrowania uprawnień

1) Dostęp do systemu informatycznego służącego do przetwarzania danych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych.
2) Podstawą do nadania uprawnień w systemie oraz dokonania wpisu w ewidencji osób upoważnionych do przetwarzania danych jest prawidłowo wypełniony imienny dokument uprawnień.
3) Imienny dokument uprawnień wykonuje Administrator Informacji. Dokument sporządzany jest również w przypadku modyfikacji lub odebrania uprawnień.
4) Dozwolone jest sporządzenie imiennego dokumentu uprawnień określającego czas obowiązywania uprawnień.
5) Rejestracja użytkownika informacji polega na nadaniu identyfikatora, przydzieleniu hasła, wprowadzeniu danych do bazy użytkowników systemu oraz wpisu do ewidencji osób upoważnionych do przetwarzania danych.

2. Procedura nadawania i rejestrowania uprawnień

1) **Administrator Informacji:**
   a) podejmuje decyzję o dopuszczeniu do przetwarzania danych osoby, która w związku z wykonywanymi przez siebie obowiązkami, zadaniami lub czynnościami będzie miała dostęp do danych i informacji,
   b) wypełnia i podpisuje dla osoby dopuszczonej do przetwarzania danych imienny dokument uprawnień (wzór - **załącznik nr 1**),
   c) przekazuje wypełniony imienny dokument uprawnień Administratorowi Bezpieczeństwa Informacji.
2) **Administrator Bezpieczeństwa Informacji** bada poprawność sporządzenia dokumentu oraz w przypadku:
   a) braku uwag przekazuje ze swoją akceptacją **Administratorowi Systemu Informatycznego** w celu nadania uprawnień użytkownikowi w systemie,
   b) uwag zwraca dokument do **Administratora Informacji**. Na dokumencie dokonuje adnotacji, w której podaje przyczynę odmowy zatwierdzenia dokumentu. Postępowanie określone w punktach 1 i 2 powtarza się do czasu uzyskania akceptacji.
3) **Administrator Systemu Informatycznego**, zgodnie z przekazanym dokumentem:
   a) nadaje użytkownikowi identyfikator i hasło,
   b) przydziela uprawnienia określone w imiennym dokumencie uprawnień,
   c) wprowadza dane do bazy użytkowników systemu,
   d) przekazuje podpisany imienny dokument uprawnień **Administratorowi Bezpieczeństwa Informacji**.
4) **Administrator Bezpieczeństwa Informacji**:
   a) dokonuje wpisu (aktualizacji) użytkownika informacji w ewidencji osób upoważnionych do przetwarzania danych,
   b) przygotowuje, dla użytkownika informacji, imienne upoważnienie do przetwarzania danych do podpisu przez **Administratora Danych**. Podpisane upoważnienie przekazuje **Administratorowi Informacji** celem podpisania przez użytkownikowi informacji oraz sporządzenia aneksu do zakresu obowiązków.

Procedurę nadania i rejestrowania uprawnień do przetwarzania danych w systemie informatycznym należy stosować odpowiednio w przypadku modyfikacji uprawnień oraz odebrania uprawnień

3. Procedura wyrejestrowania uprawnień

1) Wyrejestrowania użytkownika z systemu informatycznego dokonuje **Administrator Systemu Informatycznego** na podstawie imiennego dokumentu uprawnień sporządzonego przez **Administratora Informacji.**
2) Do odebrania uprawnień i wyrejestrowania użytkownika informacji stosuje się odpowiednio postępowanie określone w pkt. 2. ppkt. 1); ppkt. 2); ppkt. 3) i ppkt. 4),
3) Wyrejestrowanie może mieć charakter czasowy lub trwały.
4) Wyrejestrowanie następuje poprzez:
   a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
5) Czasowe wyrejestrowanie użytkownika z systemu informatycznego następuje w razie:
   a) nieobecności użytkownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
   b) naruszenia zasad i procedur pracy w systemie informatycznym,
   c) zawieszenia w pełnieniu obowiązków służbowych.
6) Przyczyną czasowego wyrejestrowania z systemu informatycznego może być:
   a) wszczęcie postępowania dyscyplinarnego wobec osoby upoważnionej do przetwarzania danych,
   b) wypowiedzenie umowy o pracy.
7) Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy albo innego stosunku prawnego.

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

1. Metody i środki uwierzytelniania

1) W systemie informatycznym stosuje się uwierzytelnienia dwustopniowe, na poziomie:
   a) dostępu do stacji roboczej,
   b) dostępu do aplikacji.
2) Do uwierzytelnienia użytkowników w systemie stosuje się identyfikatory oraz hasła.
3) Identyfikator składa się z litery odpowiadającej pierwszej literze imienia użytkownika znak „ . "(kropka) oraz kolejnym literom jego nazwiska. W identyfikatorze pomija się polskie znaki diakrytyczne.
4) W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika **Administrator Systemu Informatycznego**, za zgodą **Administratora Bezpieczeństwa Informacji**, nadaje użytkownikowi inny identyfikator, odstępując od zasady określonej wyżej.
5) Hasło na poziomie dostępu do aplikacji/systemu składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.
6) Hasło nie może być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
7) Hasło nie może być ujawnione nawet po utracie przez nie ważności.
8) Użytkownik nie może udostępniać swojego identyfikatora i hasła osobom trzecim.
9) Bezwzględnie zabronione jest korzystanie z identyfikatora i hasła innego użytkownika.
10) Zmiana hasła następuje:
    a) nie rzadziej niż co 30 dni w przypadku dostępu do aplikacji/systemów, w których przetwarzane są dane osobowe,
    b) nie rzadziej niż co 90 dni w przypadku dostępu do innych aplikacji/systemów niż wymienione wyżej,

c) niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione lub zapomnienia przez użytkownika.

11) System informatyczny umożliwia automatycznie:
   a) przypisanie wprowadzanych danych użytkownikowi (identyfikatorowi), który te dane wprowadził do systemu,
   b) sygnalizację czasu wygaśnięcia obowiązywania hasła dostępu do stacji roboczej.

2. Procedury zarządzania środkami uwierzytelniania

1) **Administrator Systemu Informatycznego** nadaje hasło dostępu do aplikacji/systemu dla nowego użytkownika albo dla użytkownika, który zapomniał swoje ostatnie hasło dostępu. Przekazywanie hasła użytkownikowi przez **Administratora Systemu Informatycznego** odbywa się w sposób poufny. Nie może ono być zapisywane w miejscu pozwalającym na dostęp osób nieupoważnionych.
2) Użytkownik dokonuje uwierzytelnienia w systemie w obecności **Administratora Systemu Informatycznego**.
3) Użytkownik systemu po pierwszym logowaniu niezwłocznie ustala swoje własne hasło, zgodnie z zasadami określonymi w punkcie 1. ppkt. 5 i 6.
4) Użytkownik systemu w trakcie pracy w aplikacji może zmieniać swoje hasło dostępu. O każdej zmianie hasła dostępu użytkownik informuje **Administratora Systemu Informatycznego.**
5) **Administrator Systemu Informatycznego** prowadzi rejestr zmian haseł użytkowników systemów/programów (wzór – **załącznik nr 2**), które automatycznie nie wymuszają zmiany hasła.
6) **Administratorowi Systemu Informatycznego**, w uzasadnionym przypadku, przysługuje prawo zablokowania konta użytkownika w każdym czasie. O zablokowaniu konta niezwłocznie informuje **Administratora Bezpieczeństwa Informacji** podając przyczyny decyzji.

VI. Procedury rozpoczęcia, zawieszenia i zakończenia pracy oraz tryb pracy

1. Procedura rozpoczęcia pracy

1) Użytkownik informacji przed rozpoczęciem lub kontynuacją pracy powinien zwrócić uwagę, czy nie istnieje prawdopodobieństwo naruszenia bezpieczeństwa przetwarzanych danych.
   Jeżeli poweźmie takie podejrzenie, musi postępować zgodnie z procedurą określoną w **punkcie XIII.**
2) Rozpoczęcie pracy w systemie informatycznym następuje po włączeniu monitora, stacji roboczej i drukarki.
3) Uruchomienie aplikacji/systemu, następuje poprzez wprowadzenie identyfikatora i hasła dostępu. Hasło dostępu należy podawać w sposób dyskretny (nie literować, nie czytać na głos). Hasło dostępu należy wprowadzać do stacji roboczej osobiście.

2. Procedura zawieszenia pracy

Użytkownik zobowiązany jest do:
1) ustawiania ręcznego blokady stacji roboczej przy każdorazowym opuszczaniu stanowiska pracy,
2) upewnienia się, że w czasie jego nieobecności, na monitorze stacji roboczej nie będą wyświetlane żadne dane i informacje.

3. Procedura zakończenia pracy

W celu zakończenia pracy użytkownik zobowiązany jest do:
1) zapisania przetwarzanych danych i informacji w odpowiednie bazy/zbiory,
2) zamknięcia aplikacji,
3) zamknięcia systemu,

4) wyłączenia monitora, drukarki i stacji roboczej.

Przed opuszczeniem pomieszczenia użytkownik informacji musi:

1) zniszczyć w niszczarce lub schować do szaf zamykanych na klucz wszelkie wykonane wydruki zawierające dane i informacje (metoda czystego biurka),
2) schować do zamykanych na klucz szaf wszelkie akta zawierające dane i informacje,
3) umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,
4) zamknąć okna.

Opuszczając pokój należy drzwi zamknąć na klucz. Klucz oddać do przechowania w ustalonym miejscu.

4. Tryb pracy na stacjach roboczych (stacjonarnych)

1) W pomieszczeniu, w którym przetwarzane są dane, osoby postronne mogą znajdować się tylko za zgodą i w obecności użytkownika informacji.
2) Należy chronić ekrany stacji roboczych (ustawienie monitora uniemożliwiające pogląd) oraz wydruki znajdujące się na biurku i w otwartych szafach przed osobami postronnymi.
3) Zakazuje się robienia kopii całych zbiorów danych przez użytkowników informacji. Całe zbiory danych mogą być kopiowane tylko przez **Administratora Systemu Informatycznego** lub automatycznie przez system, z zachowaniem procedur ich ochrony.
4) Jednostkowe dane mogą być kopiowane na zewnętrzne nośniki magnetyczne i optyczne. Nośniki te są przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane.
5) Przesyłanie danych pocztą elektroniczną może odbywać się tylko w postaci zaszyfrowanej.
6) Jednostkowe dane mogą być przekazywane pocztą elektroniczną pomiędzy stacjami roboczymi **Administratora Danych**, a komputerami przenośnymi użytkowników informacji tylko po ich zaszyfrowaniu.
7) Zakazuje się wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej.
8) Użytkownicy informacji zobowiązani są do odpowiednio częstego robienia kopii roboczych przetwarzanych danych i informacji, na których właśnie pracują, aby zapobiec ich utracie.

5. Tryb pracy na komputerach przenośnych

1) Przy przetwarzaniu danych i informacji na komputerach przenośnych bezwzględnie obowiązują procedury określone w niniejszej instrukcji.
2) Użytkownicy informacji, którym zostały powierzone komputery przenośne, zobowiązani są chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych. Szczególną ostrożność należy zachować podczas ich transportu.
3) Zakazuje się używania komputerów przenośnych przez osoby inne niż użytkownicy informacji, którym zostały one powierzone,
4) Praca na komputerze przenośnym możliwa jest po wprowadzeniu indywidualnego identyfikatora i hasła użytkownika informacji.
5) Użytkownicy informacji są zobowiązani do zmiany hasła w komputerach przenośnych nie rzadziej niż raz na 30 dni,
6) Pliki zawierające dane i informacje przechowywane na komputerach przenośnych powinny być zaszyfrowane i opatrzone hasłem dostępu,
7) Zakazuje się przetwarzania na komputerach przenośnych całych zbiorów danych lub szerokich z nich wypisów, nawet w postaci zaszyfrowanej.
8) Użytkownicy informacji przetwarzający dane i informacje na komputerach przenośnych zobowiązani są do systematycznego wprowadzania (kopiowania) tych danych i informacji w określone przez **Administratora Danych**, odpowiednie bazy/zbiory, a następnie do trwałego ich usuwania z pamięci powierzonych komputerów przenośnych.
9) Komputery przenośne wyposażone są w odpowiednie programy ochrony antywirusowej.

10) Zakazuje się samodzielnej modernizacji oprogramowania i sprzętu powierzonych komputerów przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem **Administratora Systemu Informatycznego,** stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to **Administratorowi Systemu Informatycznego**.

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

1) **Administrator Systemu Informatycznego** prowadzi rejestr wykonanych kopii zapasowych, sprawuje nadzór nad ich wykonywaniem oraz weryfikuje ich poprawność (wzór – **załącznik nr 4**).
2) W celu sprawdzenia poprawności wykonywanych kopii **Administrator Systemu Informatycznego** poddaje testowi wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych.
3) **Administrator Bezpieczeństwa Informacji** sporządza wykaz informacji chronionych. Dane te oraz dane przechowywane w pamięci stacji roboczych archiwizowane są w cyklu określonym przez **Administratora Systemu Informatycznego** na odpowiednich nośnikach informatycznych.
4) **Administratorzy Informacji** dokonują oceny danych przechowywanych w pamięci stacji roboczych pod kątem ich ważności dla obsługi interesantów oraz funkcjonowania Urzędu Gminy Mała Wieś, kwalifikują je jako informacje chronione oraz zobowiązują pisemnie użytkowników informacji (pracowników) do ich kopiowania w sposób określony w punktach 5, 6, 7 i 8 (wzór – **załącznik nr 6**).
5) **Użytkownicy informacji** są zobowiązani do wykonywania kopi zapasowych swoich danych i informacji przechowywanych w pamięci stacji roboczych oraz programów i narzędzi programowych, w sposób określony przez **Administratora Systemu Informatycznego**.
6) Kopie zapasowe, o których mowa w pkt. 5 tworzy się:
   a) codziennie – na koniec dnia kopię wszystkich danych, które uległy zmianie tego dnia,
   b) raz w tygodniu – na koniec tygodnia kopię wszystkich danych bez względu czy uległy zmianie czy nie.
7) Dopuszcza się tworzenie kopii zapasowych (archiwalnych) na innych, oddzielnych nośnikach informacji.
8) Dostęp do kopii zapasowych posiada **Administrator Systemu Informatycznego** oraz **Administrator Bezpieczeństwa Informacji**.
9) Kopie czasowe tworzy się na oddzielnych nośnikach informatycznych zgodnie z zasadami określonymi w Rozdziale VI, pkt.5) Polityki Bezpieczeństwa.

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

1. Elektroniczne nośniki informacji

1) Dane w postaci elektronicznej przetwarzane w systemach informatycznych, zapisane na dyskietkach, dyskach magnetooptycznych, dyskach twardych, pendrivach itp. nie mogą być wynoszone poza siedzibę Urzędu Gminy Mała Wieś bez zgody **Administratora Danych.**
   Fakt przetwarzania danych poza siedzibą Urzędu Gminy Mała Wieś musi być odnotowany w prowadzonej ewidencji (wzór – **załącznik nr 7**).
2) Wymienne, elektroniczne nośniki informacji przechowywane są w pokojach stanowiących obszar przetwarzania danych, określonych w Zarządzeniu Nr 219/89 /2016 Wójta Gminy Mała Wieś z dnia 17 listopada 2016 roku w sprawie Polityki

Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Mała Wieś. Po zakończeniu pracy są zabezpieczane przez użytkowników informacji w zamykanych w szafach biurowych lub kasetkach.

3) Z danych przetwarzanych w pamięci stacji roboczych oraz komputerów przenośnych muszą być bezwzględnie wykonywane kopie zapasowe na odpowiednich nośnikach informacji, zgodnie z procedurami określonymi w Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym.
4) Dane w postaci elektronicznej należy usunąć z nośnika informacji w sposób uniemożliwiający ich ponowne odtworzenie, nie później niż po upływie 3 dni, po wykorzystaniu tych danych chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania. O usunięciu danych decyduje **Administrator Danych** lub **Administrator Informacji**.
5) W przypadku uszkodzenia lub zużycia nośnik, zawierający dane, należy zniszczyć fizycznie w taki sposób, by nie można było odczytać jego zawartości (w niszczarce służącej do niszczenia nośników, przecięcia lub przełamania).
6) Urządzenia, dyski lub inne elektroniczne nośniki informacji przeznaczone do naprawy muszą być pozbawione danych w sposób uniemożliwiający ich odzyskanie lub być naprawiane pod nadzorem **Administratora Systemu Informatycznego**.
7) Urządzenia, dyski i inne elektroniczne nośniki informacji przeznaczone do przekazania podmiotowi nieuprawnionemu do przetwarzania danych na nich zawartych muszą być wcześniej pozbawione zapisu tych danych w sposób uniemożliwiający ich odzyskanie.
8) Urządzenia, dyski oraz inne elektroniczne nośniki informacji przeznaczone do likwidacji muszą być pozbawione zapisów lub trwale uszkodzone w sposób uniemożliwiający odczytanie z nich danych. Likwidacja prowadzona jest zgodnie z obowiązującymi w Urzędzie Gminy Mała Wieś przepisami dotyczącymi gospodarki środkami trwałymi oraz wartościami niematerialnymi.

2. Kopie zapasowe

1) Kopie zapasowe, wykonywane zgodnie z procedurą określoną w Rozdziale VII, zbiorów danych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w szafie metalowej.
2) Zabronione jest przechowywanie kopii zapasowych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.
3) Dostęp do szafy, w której są przechowywane kopie zapasowe, mają tylko osoby upoważnione, tj. **Administrator Bezpieczeństwa Informacji** oraz **Administrator Systemu Informatycznego**.
4) Kopie zapasowe powinny być przechowywane w pomieszczeniu, z zainstalowanym systemem wykrywania pożaru.
5) Kopie zapasowe likwiduje się niezwłocznie po ustaniu ich użyteczności.

3. Wydruki

1) Wydruki zawierające dane są przechowywane w zamkniętych szafach, w pokojach stanowiących obszar przetwarzania danych, określonych w Zarządzeniu Nr 219/89/2016 Wójta Gminy Mała Wieś z dnia 17 listopada 2016 roku w sprawie Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Mała Wieś.
2) Wydruki zawierające dane należy zniszczyć przez pocięcie w specjalnym urządzeniu /niszczarce/ nie później niż po upływie 3 dni, po ich wykorzystaniu chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania. O zniszczeniu wydruków decyduje **Administrator Danych** lub **Administrator Informacji**.

4. Dane wejściowe do systemu

1) Dane zapisane w formie papierowej, innej niż wydruki z systemów (pisma, ankiety, formularze itp.), są przechowywane na tych samych zasadach jak wydruki.
2) Formularze zgody z podpisami osób, których dotyczą dane przetwarzane w systemach, przechowywane są w pokojach stanowiących obszar przetwarzania danych, określonych w Zarządzeniu Nr 219/89/2016 Wójta Gminy Mała Wieś z dnia 17 listopada 2016 roku w sprawie Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Mała Wieś.
3) Z danymi zapisanymi w formie elektronicznej należy postępować odpowiednio, w sposób opisany, w rozdziale VI, pkt.5 Polityki Bezpieczeństwa.

IX. Środki ochrony systemów przed złośliwym oprogramowaniem, w tym wirusami komputerowymi i nieuprawnionym dostępem

1. Ochrona antywirusowa

1) Działanie ochrony antywirusowej systemów informatycznych nadzoruje **Administrator Systemu Informatycznego**. Do jego obowiązków należy określenie częstotliwości automatycznych aktualizacji definicji wirusów dokonywanych przez oprogramowanie antywirusowe, zapewnienie prawidłowego funkcjonowania ochrony antywirusowej systemu informatycznego oraz aktualizacja oprogramowania antywirusowego.
2) Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na stacjach roboczych oraz komputerach przenośnych.
3) Użytkownik informacji jest obowiązany zawiadomić **Administratora Systemu Informatycznego** o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
4) W celu zapewnienia właściwej ochrony przed wirusami komputerowymi używanie nośników danych (dyskietki, dyski optyczne itp.) spoza Urzędu Gminy Mała Wieś jest dopuszczalne dopiero po uprzednim sprawdzeniu ich przy pomocy programu antywirusowego. Jeżeli stanowisko użytkownika informacji nie jest wyposażone w program antywirusowy, nośnik danych należy przekazać do sprawdzenia przez **Administratora Systemu Informatycznego.**
5) W przypadku stwierdzenia obecności wirusów komputerowych w systemie należy postępować w sposób opisany w punkcie XIII.
6) Użytkownik systemu na stanowisku komputerowym, importujący dane do systemu informatycznego jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów.

2. Ochrona przed nieautoryzowanym dostępem, bezpieczeństwo i zasady pracy w sieci komputerowej

1) Zasoby informatyczne użytkownikom informacji udostępnia **Administrator Systemu Informatycznego**.
2) Urządzenia systemu informatycznego służącego do przetwarzania danych ważnych dla obsługi mieszkańców i funkcjonowania Urzędu Gminy Mała Wieś mogą być połączone z siecią Internet.
3) Na stanowiskach komputerowych mających dostęp do Internetu musi być zainstalowane oprogramowanie antywirusowe oraz zainstalowany program Firewall.
4) Korzystanie z Internetu jest możliwe tylko w przypadku, jeżeli jest to niezbędne do wykonywania obowiązków służbowych.
5) ***Zabronione jest otwieranie załączników poczty elektronicznej nieznanego typu oraz pochodzące z podejrzanej lub nieznanej korespondencji.***
6) Użytkownikowi informacji pod żadnym pozorem nie wolno zmieniać adresu IP i innych parametrów urządzeń komunikacji sieciowej.

7) Użytkownik informacji jest zobowiązany do ścisłego przestrzegania zasad pracy w sieci określonych w Polityce Bezpieczeństwa i Rozdziale V, pkt. 1. Instrukcji Zarządzania Systemem Informatycznym.

X. Zasady i sposób odnotowywania w systemach informacji o udostępnieniu danych

1) Bezpośredni nadzór nad udostępnianiem danych sprawuje **Administrator Informacji**. Natomiast nadzór nad prawidłowością udostępniania danych sprawuje **Administrator Bezpieczeństwa Informacji.**
2) Udostępnienie danych może nastąpić wyłącznie na wniosek odbiorcy danych zgodnie z zasadami określonymi w Polityce Bezpieczeństwa.
3) Odbiorcą danych jest każdy, komu udostępnia się dane, z wyłączeniem:
   a) osoby, której dane dotyczą,
   b) osoby użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych w Urzędzie Gminy Mała Wieś,
   c) przedstawiciela, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych,
   d) podmiotu, któremu powierzono przetwarzanie danych,
   e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
4) Odnotowanie obejmuje informacje o:
   a) nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
   b) zakresie udostępnianych danych,
   c) dacie udostępnienia,
5) Obowiązek odnotowania wyżej wymienionych informacji spoczywa na użytkowniku informacji poprzez wypełnienie odpowiednich pól w bazie danych.
6) Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.
7) W systemie informatycznym odnotowywane są informacje o odbiorcach danych z tego systemu.
8) Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnieniu danych należy umieścić w raporcie z systemu informatycznego, a raport przekazać tej osobie.
9) W przypadku braku możliwości odnotowywania przez system informatyczny udostępnienia danych, informację o tym należy zamieścić w ewidencji udostępniania danych prowadzonej w formie papierowej lub elektronicznej (wzór - **załącznik 8**).

XI. Procedury wykonywania napraw urządzeń oraz przeglądów i konserwacji systemów, w tym elektronicznych nośników informacji służących do przetwarzania danych

O przeprowadzanych przeglądach i konserwacjach systemu w każdym przypadku informowany jest **Administrator Bezpieczeństwa Informacji**, który może być przy nich obecny. **Administrator Bezpieczeństwa Informacji** może przeprowadzać kontrole i testy obejmujące zarówno dostęp do zasobów systemów, jak i profile oraz uprawnienia poszczególnych użytkowników informacji.

1. Przeglądy i konserwacja urządzeń

1) Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonym przez producenta sprzętu.
2) Ocenie podlegają: stan techniczny urządzeń (komputery, serwery, UPS-y, itp.), stan okablowania budynku w sieć logiczną, spójność baz danych, stan rejestrów systemów serwera lokalnej sieci komputerowej.

3) Nieprawidłowości ujawnione w trakcie przeglądów i konserwacji powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić **Administratora Bezpieczeństwa Informacji**.
4) Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada **Administrator Systemu Informatycznego**.

2. Przegląd programów i narzędzi programowych

1) Przeglądu pliku zawierającego raport dotyczący działania aplikacji bądź systemu (log systemowy) dokonuje **Administrator Systemu Informatycznego** nie rzadziej niż raz na miesiąc. Zapisy logów systemowych są przeglądane przez **Administratora Systemu Informatycznego** każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.
2) Przeglądu i sprawdzenia poprawności zbiorów danych dokonuje użytkownik przy współudziale **Administratora Systemu Informatycznego**.
3) Przegląd programów i narzędzi programowych przeprowadzany jest w następujących przypadkach:
   a) zmiany wersji oprogramowania stacji roboczej użytkownika systemu,
   b) zmiany systemu operacyjnego stacji roboczej użytkownika systemu,
   c) wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.
4) Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych. Sprawdzenie powinno obejmować:
   a) poprawność logowania się do systemu w zależności od posiadanych uprawnień (symulacja pracy wszystkich typów uprawnień użytkownika),
   b) poprawność działania wszystkich elementów aplikacji (menu, zestawienia, formularze, raporty),
   c) poprawność funkcjonalną systemu, z symulacją działania wszystkich grup użytkowników przy wykonaniu następujących operacji:
      ✓ wprowadzanie danych,
      ✓ edytowanie danych,
      ✓ wyszukiwanie danych,
      ✓ wydruku danych.
5) Przegląd przeprowadza projektant systemu w obecności **Administratora Systemu Informatycznego**.
6) Prawidłowy przebieg przeprowadzenia przeglądu programów i narzędzi programowych systemów nadzoruje **Administrator Systemu Informatycznego**.

3. Zarządzanie oprogramowaniem systemowym i użytkowym

1) Nośniki informatyczne zakupionego oprogramowania operacyjnego, narzędziowego i aplikacyjnego przechowywane są w chronionym i zabezpieczonym przed nieuprawnionym dostępem miejscu.
2) **Administrator Systemu Informatycznego** prowadzi rejestr oprogramowania z oznaczeniem użytkowników informacji, którym zostało ono udostępnione (wzór - **załącznik nr 3**).
3) Użytkownik może korzystać z udostępnionego oprogramowania jedynie w celu wykonywania obowiązków służbowych.
4) Zabronione jest wykonywanie przez użytkownika jakichkolwiek instalacji oprogramowania bez zgody **Administratora Systemu Informatycznego**.
5) Użytkownikowi nie wolno dokonywać jakichkolwiek zmian w konfiguracji systemu operacyjnego.

4. Konserwacja oprogramowania

1) Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu potrzeby wprowadzenia zmian pozwalających utrzymać funkcjonalność systemu w dynamicznie zmieniającym się środowisku pracy.
2) Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych, na testowej bazie danych, stosując odpowiednio zasady określone dla przeglądu oprogramowania.
3) Konserwacja przeprowadzana jest w obecności **Administratora Systemu Informatycznego**.

5. Naprawa urządzeń

1) Naprawa urządzeń komputerowych oraz zmiany w systemach informatycznych przeprowadzane są pod nadzorem **Administratora Systemu Informatycznego**.
2) Naprawa urządzeń oraz zmiany w systemie informatycznym wykonywane przez serwisanta w siedzibie Urzędu Gminy Mała Wieś mogą być prowadzone tylko zgodnie z zasadami określonymi w rozdziale VI, pkt. 3 Polityki Bezpieczeństwa.
3) Naprawy urządzeń poza siedzibą Urzędu Gminy Mała Wieś mogą być dokonywane po spełnieniu warunków określonych w rozdziale VI, pkt. 3 Polityki Bezpieczeństwa.

XII. Przetwarzanie danych w zbiorach doraźnych

1) Dostęp do danych odbywa się poprzez aplikacje. Gdy zachodzi potrzeba zapisania danych w innym formacie np. dane do raportu w postaci pliku arkusza kalkulacyjnego, można tego dokonać w doraźnym zbiorze danych pod warunkiem, zapewnienia danym należytej ochrony, tj.:
   a) uniemożliwienia dostępu do danych osobom nieuprawnionym,
   b) uniemożliwienia zmiany danych, a tym samym sfałszowania informacji pochodzących z systemu,
   c) zabezpieczenia bezpośredniego dostępu do danych hasłem.
2) Zbiór danych doraźnych można zapisać na dysku stacji roboczej bądź innym elektronicznym nośniku informacji postępując zgodnie z procedurą określoną w Rozdziale VI, pkt. 5 Polityki Bezpieczeństwa.
3) Doraźny zbiór danych należy usunąć z nośnika danych, na którym został utworzony lub zniszczyć nośnik, nie później niż 3 dni po wykorzystaniu danych. O usunięciu danych lub nośnika decyduje **Administrator Informacji.**
4) Dane w zbiorach doraźnych mogą być przetwarzane wyłącznie w pomieszczeniach chronionych wchodzących w skład obszaru ochrony przetwarzanych danych i informacji. W przypadku konieczności przetwarzania danych w zbiorach doraźnych poza tymi pomieszczeniami należy bezwzględnie stosować procedurę określoną w Rozdziale VIII, pkt.1.
5) W przypadku podejrzenia lub stwierdzenia nieuprawnionego dostępu do danych w zbiorze doraźnym należy niezwłocznie zawiadomić Administratora Bezpieczeństwa Informacji oraz postępować zgodnie z procedurą określoną w Rozdziale XIII.

XIII. Postępowanie w przypadku stwierdzenia naruszenia zasad bezpieczeństwa przetwarzanych danych w systemie informatycznym

Natychmiastowe podjęcie działań przez osoby odpowiedzialne ma na celu zabezpieczenie systemu informatycznego w przypadku naruszenia jego zabezpieczeń czy zmian w sposobie działania programu lub urządzeń, wskazujących na naruszenie bezpieczeństwa danych. Podjęte działania mają na celu wykrycie przyczyny lub sprawcy zaistniałej sytuacji oraz jej usunięcie.

1) Domniemanie, przesłanka czy fakt wskazujące na naruszenie zasad ochrony danych, a zwłaszcza stan różny od ustalonego w systemie informatycznym, jest dla użytkownika informacji podstawą do podjęcia natychmiastowego działania.

2) O sytuacji odbiegającej od normy, w szczególności o przesłankach naruszenia lub podejrzenia naruszenia zasad ochrony danych w systemie informatycznym, użytkownik zobowiązany jest natychmiast poinformować **Administratora Bezpieczeństwa Informacji** oraz **Administratora Systemu Informatycznego**, a zwłaszcza o:
   a) naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła),
   b) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
   c) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów,
   d) wykryciu wirusa komputerowego,
   e) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego,
   f) znacznym spowolnieniu działania systemu informatycznego,
   g) faktach świadczących o działaniu systemu poza dozwolonym czasem pracy,
   h) stanie aktywnych urządzeń sieciowych i pozostałej infrastruktury informatycznej,
   i) stanie urządzeń (brak zasilania, problemy z uruchomieniem),
   j) zmianie położenia sprzętu komputerowego,
   k) podejrzeniu próby kradzieży sprzętu komputerowego lub dokumentów z danymi,
   l) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf,
   m) stanie systemu zabezpieczenia pomieszczenia/obiektu (urządzenia alarmowe itp.),
   n) przebywaniu osób nieuprawnionych w pomieszczeniach chronionych obszaru przetwarzania danych,
   o) wystąpieniu nieprzewidzianej sytuacji losowej związanej z zalaniem pomieszczeń z uszkodzonych elementów sieci centralnego ogrzewania lub wodociągowej.
3) Do czasu przybycia na miejsce zdarzenia **Administratora Systemu Informatycznego** użytkownik stwierdzający naruszenie przepisów lub stan mogący mieć wpływ na bezpieczeństwo danych i systemu zobowiązany jest do pełnego udokumentowania zdarzenia (np. zapisania treści komunikatów), celem precyzyjnego określenia przyczyn i ewentualnych skutków naruszenia obowiązujących zasad, a w szczególności:
   a) niezwłocznego podjęcia czynności niezbędnych dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnienia w działaniu również ustalenia jego przyczyn lub sprawców,
   b) wstrzymania bieżącej pracy na stacji roboczej lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   c) zaniechania planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
   d) zastosowania się do instrukcji i regulaminów lub dokumentacji urządzeń, jeśli odnoszą się one do zaistniałego przypadku,
   e) przygotowania opisu incydentu,
   f) nie opuszczania, bez uzasadnionej przyczyny, miejsca zdarzenia do czasu przybycia **Administratora Systemu Informatycznego**.
4) Stwierdzenie przez **Administratora Systemu Informatycznego** naruszenia zasad ochrony danych wymaga bezzwłocznego powiadomienia **Administratora Bezpieczeństwa Informacji** oraz podjęcia natychmiastowych działań poprzez:
   a) usunięcie stwierdzonych uchybień (np. wymiana niesprawnego zasilacza awaryjnego, usunięcie wirusów z systemu komputerowego, itp.),
   b) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane,
   c) wstrzymanie przetwarzania danych do czasu całkowitego usunięcia awarii systemu informatycznego oraz zakończenia działań zabezpieczających system informatyczny.
5) **Administrator Bezpieczeństwa Informacji** po otrzymaniu zawiadomienia o incydencie podejmuje niezwłocznie:

a) postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia zabezpieczeń ochrony danych, wykrycia przyczyny lub sprawcy zaistniałej sytuacji,
b) działania w celu jej usunięcia,
c) działania chroniące system przed ponownym naruszeniem.

6) **Administrator Bezpieczeństwa Informacji** w uzgodnieniu z **Administratorem Systemu Informatycznego** może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.
7) W przypadku odtwarzania danych z kopii zapasowych **Administrator Systemu Informatycznego** obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu (dotyczy to zwłaszcza przypadków infekcji wirusowej).
8) W przypadku stwierdzenia naruszenia bezpieczeństwa danych lub systemu informatycznego **Administrator Bezpieczeństwa Informacji/Administrator Systemu Informatycznego** sporządza raport naruszenia bezpieczeństwa (wzór - **załącznik nr 5**), a następnie niezwłocznie przekazuje go **Administratorowi Danych**.
9) W przypadku podejrzenia, iż naruszenie bezpieczeństwa danych spowodowane zostało zaniedbaniem lub naruszeniem dyscypliny pracy, **Administratora Bezpieczeństwa Informacji** przedstawia **Administratorowi Danych** wniosek o wszczęcie postępowania wyjaśniającego oraz ukaranie osób odpowiedzialnych.
10) **Administrator Danych** po zapoznaniu się z raportem naruszenia bezpieczeństwa danych lub systemu informatycznego oraz wnioskami **Administratora Bezpieczeństwa Informacji** podejmuje decyzje o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych czynności zapewniających bezpieczeństwo danych lub systemu informatycznego lub zastosowaniu środków ochrony fizycznej.
11) **Administrator Bezpieczeństwa Informacji** i **Administrator Systemu Informatycznego** zobowiązani są do informowania **Administratora Danych** o awariach systemu informatycznego, stwierdzonych przypadkach naruszenia Instrukcji Zarządzania Systemem Informatycznym przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego korzystania ze sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.

Postępowanie w przypadku naruszenia zasad bezpieczeństwa przetwarzanych danych w systemie informatycznym stosuje się odpowiednio w przypadku naruszenia zasad bezpieczeństwa przetwarzanych danych w systemie tradycyjnym

XIV. Postanowienia końcowe

1) W sprawach nieuregulowanych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
2) Osoby upoważnione do przetwarzania danych zobowiązane są do zapoznania się, przed dopuszczeniem do przetwarzania danych, z niniejszą instrukcją oraz złożenia stosownego oświadczenia, potwierdzającego znajomość jej treści.
3) Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym na podstawie Kodeksu Pracy.
4) Osoby naruszające zasady i procedury określone w Instrukcji Zarządzania Systemem Informatycznym będą pociągnięte do odpowiedzialności karnej, na podstawie art. 51-52 ustawy oraz art. 266 Kodeksu Karnego.

Instrukcja Zarządzania Systemem Informatycznym wchodzi w życie z dniem 17 listopada 2016 roku.

Dokument powiązany: ***Polityka Bezpieczeństwa w Urzędzie Gminy Mała Wieś.***

Załączniki:
Załącznik nr 1 – Imienny Dokument Uprawnień
Załącznik nr 2 – Rejestr zmian hasła użytkownika systemu/programu
Załącznik nr 3 – Rejestr udostępnionego oprogramowania
Załącznik nr 4 – Rejestr kopii zapasowych (bezpieczeństwa) danych
Załącznik nr 5 – Raport naruszenia bezpieczeństwa danych/systemu informatycznego w Urzędzie Gminy Mała Wieś
Załącznik nr 6 – Wykaz danych do archiwizacji w Urzędzie Gminy Mała Wieś
Załącznik nr 7 – Ewidencja przetwarzania danych poza siedzibą Urzędu Gminy Mała Wieś
Załącznik nr 8 – Ewidencja udostępniania danych w Urzędzie Gminy Mała Wieś

Załącznik nr 1

Imienny Dokument Uprawnień

□ *Nowy użytkownik*	□ *Modyfikacja uprawnień*	□ *Odebranie uprawnień*
Imię i nazwisko użytkownika:	**Komórka organizacyjna:**	
Stanowisko:	**Pokój nr:**	**Telefon nr:**

Nazwa systemu/programu	**Zakres uprawnień**
1. Dostęp do stacji roboczej	**forma papierowa** □ przetwarza dane osobowe □ zbieranie □ przechowywanie □ zmienianie □ usuwanie □ opracowywanie □ przekazywanie □ kopiowanie **forma elektroniczna** □ przetwarza dane osobowe □ zbieranie □ przechowywanie □ zmienianie □ usuwanie □ opracowywanie □ przekazywanie □ kopiowanie
Login:	
2.	**forma papierowa** □ przetwarza dane osobowe □ zbieranie □ przechowywanie □ zmienianie □ usuwanie □ opracowywanie □ przekazywanie □ kopiowanie **forma elektroniczna** □ przetwarza dane osobowe □ zbieranie □ przechowywanie □ zmienianie □ usuwanie □ opracowywanie □ przekazywanie □ kopiowanie
Login:	
3.	**forma papierowa** □ przetwarza dane osobowe □ zbieranie □ przechowywanie □ zmienianie □ usuwanie □ opracowywanie □ przekazywanie □ kopiowanie **forma elektroniczna** □ przetwarza dane osobowe □ zbieranie □ przechowywanie □ zmienianie □ usuwanie □ opracowywanie □ przekazywanie □ kopiowanie
Login:	

Zasady zastępstwa i/lub okres ważności uprawnień:

Administrator Informacji Data i podpis	*Administrator Systemów Informatycznych* Data i podpis
Upoważnienie Nr...../...	*Administrator Bezpieczeństwa Informacji* Data i podpis

Załącznik nr 2

Rejestr zmian hasła użytkownika systemu/programu

System/program: .....

Pracownik: .....

Identyfikator: .....

Data rejestracji: .....

Data wyrejestrowania: .....

Lp.	Data	Przyczyna zmiany	Podpis Administratora Systemu Informatycznego	Podpis użytkownika	Uwagi
1	**2**	**3**	**4**	**5**	**6**

Załącznik nr 3

Rejestr udostępnionego oprogramowania

Użytkownik: .....

Stanowisko: .....

L.p.	Nazwa programu	Data udostępnienia	Data wycofania prawa do programu	Podpis Administratora Systemu Informatycznego	Podpis użytkownika	Uwagi
1	**2**	**3**	**4**	**5**	**6**	**7**

Załącznik nr 4

Rejestr kopii zapasowych danych

System/program: .....

Komputer/lokalizacja: .....

Nośnik kopii: .....

Miejsce przechowywania: .....

Lp.	Data wykonania kopii	Data następnej archiwizacji	Podpis Administratora Systemu Informatycznego	Uwagi
1	**2**	**3**	**4**	**5**

Załącznik nr 5

RAPORT
naruszenia bezpieczeństwa danych/systemu informatycznego w Urzędzie Gminy Mała Wieś

1. Data: ..... Godzina: .....
2. Osoba powiadamiająca o zaistniałym zdarzeniu/incydencie:

   .....
   (imię, nazwisko, stanowisko służbowe, nazwa użytkownika (login))
3. Lokalizacja zdarzenia:

   .....
   (komórka organizacyjna, nr/nazwa pomieszczenia)
4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące naruszeniu:

   .....

   .....

   .....

   .....

   .....
5. Przyczyny wystąpienia zdarzenia/incydentu:

   .....

   .....

   .....

   .....
6. Podjęte działania:

   .....

   .....

   .....

   .....
7. Postępowanie wyjaśniające/wnioski:

   .....

   .....

   .....

   .....

....

(data, podpis Administratora Systemu Informatycznego)

(data, podpis Administratora Bezpieczeństwa Informacji)

Załącznik nr 6

WYKAZ
danych do archiwizacji
w Urzędzie Gminy Mała Wieś

Lp.	Data	Nazwa zbioru/rejestru	Imię i nazwisko użytkownika informacji	Podpis użytkownika informacji	Podpis Administratora Bezpieczeństwa Informacji	UWAGI
1	2	3	4	5	6	7

Załącznik nr 7

EWIDENCJA
przetwarzania danych poza siedzibą Urzędu Gminy Mała Wieś

Lp.	Data	Nazwa zbioru/rejestru z którego dane będą przetwarzane poza siedzibą Urzędu Gminy Mała Wieś	Imię i nazwisko użytkownika informacji	Nośnik informacji zawierający dane	Podpis użytkownika informacji	Podpis Administratora Danych	UWAGI
1	2	3	4	5	6	7	8

Załącznik nr 8

EWIDENCJA UDOSTĘPNIANYCH DANYCH
w Urzędzie Gminy Mała Wieś

Lp.	Nazwa i adres podmiotu któremu udostępniono dane	Data udostępnienia	Zakres udostępnionych danych	Nazwa zbioru, rejestru, programu	Login/imię i nazwisko użytkownika informacji udostępniającego dane	UWAGI
1	2	3	4	5	6	7