WÓJT GMINY
MAŁA WIEŚ

Zarządzenie 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

Na podstawie art. 3 ust. 1, art. 7 pkt. 4 i art. 36 ust. 1 i 3 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U. z 2016 roku poz. 922) oraz art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (t.j. Dz.U. z 2016 roku poz. 446 z późn. zm.) zarządza się co następuje:

§ 1

1. Administratorem Danych jest Wójt Gminy Mała Wieś.

§ 2

1. Do przetwarzania danych osobowych w Urzędzie Gminy Mała Wieś dopuszcza się wyłącznie osoby posiadające pisemne upoważnienie Administratora Danych.
2. Do obszarów i pomieszczeń przetwarzania danych dopuszcza się wyłącznie osoby posiadające pisemne imienne upoważnienie Administratora Danych do dostępu do tych obszarów i pomieszczeń.

§ 3

1. Administratorem Bezpieczeństwa Informacji w Urzędzie Gminy Mała Wieś jest **Kamil Bernacki** – Podinspektor ds. zarządzania kryzysowego, obrony cywilnej i spraw obronnych, ochrony informacji niejawnych, ochrony danych osobowych i ochrony ppoż. - podlegający bezpośrednio Wójtowi Gminy Mała Wieś.
2. Administratorem Systemu Informatycznego jest **Adam Kacprzak** - Pomoc administracyjna.
3. Obowiązki Administratora Bezpieczeństwa Informacji, Administratora Systemu Informatycznego, użytkowników informacji oraz innych elementów systemu bezpieczeństwa określa Polityka Bezpieczeństwa w Urzędzie Gminy Mała Wieś.

§ 4

Zobowiązuje się wszystkich pracowników Urzędu Gminy Mała Wieś do:

1. Współdziałania z Administratorem Bezpieczeństwa Informacji w zakresie przestrzegania zasad ochrony przetwarzanych danych osobowych wynikających z Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym.
2. Współdziałania z Administratorem Systemu Informatycznego w zakresie funkcjonowania systemów informatycznych.

§ 5

Traci moc Zarządzenie Nr 66/51/2015 Wójta Gminy Mała Wieś z dnia 23 czerwca 2015 w sprawie wykonywania ustawy o ochronie danych osobowych w Urzędzie Gminy Mała Wieś.

§ 6

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji w Urzędzie Gminy Mała Wieś.

§ 7

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Zygmunt Wojnaro

Załącznik Nr 1
do Zarządzenia nr 218/88/2016
Wójta Gminy Mała Wieś
z dnia 17 listopada 2016 roku

P O L I T Y K A

B E Z P I E C Z E Ń S T W A

Spis treści

Wstęp **3**
I. Postanowienia ogólne 3
1. Definicje 3
2. Cel 5
3. Zakres stosowania 5
II. Organizacja przetwarzania danych 5
1. Administrator Danych 5
2. Administrator Bezpieczeństwa Informacji 6
3. Administrator Systemów Informatycznych 6
4. Administrator Informacji 7
5. Użytkownik Informacji upoważniony do przetwarzania danych i informacji 8
6. Osoby zobowiązane do zabezpieczenia danych i informacji 9
III. Infrastruktura przetwarzania danych osobowych 10
1. Obszar ochrony przetwarzania danych i informacji 10
2. Zbiory danych przetwarzane w systemach tradycyjnych i informatycznych 10
IV. Struktura zbiorów przetwarzanych w systemach 10
V. Przepływ danych pomiędzy poszczególnymi systemami eksploatowanymi w Urzędzie Gminy Mała Wieś 10
VI. Strategia zabezpieczenia danych oraz środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności danych i informacji przetwarzanych w systemach funkcjonujących w Urzędzie Gminy Mała Wioeś 11
1. Bezpieczeństwo osobowe 11
2. Strefy bezpieczeństwa 12
3. Zabezpieczenie sprzętu stosowane przez Administratora Danych 14
4. Zasady zabezpieczeń stosowane przez osoby upoważnione 15
5. Postępowanie z nośnikami i ich bezpieczeństwo 16
6. Wymiana danych i ich bezpieczeństwo 17
7. Udostępnianie danych osobowych 17
8. Kontrola dostępu do systemów 18
9. Kontrola dostępu do sieci 18
10. Komputery przenośne i praca na odległość 19
11. Monitorowanie dostępu do systemów i ich użycia 19
12. Przeglądy okresowe zapobiegające naruszeniom obowiązku szczególnej staranności Administratora Danych 20
13. Szkolenia w zakresie ochrony danych 20
14. Odpowiedzialność osób upoważnionych do przetwarzania danych 21
15. Zastosowane środki techniczne i organizacyjne 21
VII. Przeglądy polityki bezpieczeństwa i audyty systemów 23
VIII. Postanowienia końcowe 24

Wstęp

Administrator Danych dołoży wszelkich starań celem zapewnienia bezpieczeństwa danych i informacji w Urzędzie Gminy w Małej Wsi. Świadom wagi zagrożeń, w tym zwłaszcza danych osobowych, deklaruje gotowość podejmowania wszelkich koniecznych działań zapobiegających możliwym zagrożeniom, między innymi takim jak:

1. sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemów przetwarzania jak: pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, działania terrorystyczne, niepożądana ingerencja ekipy remontowej lub innych osób przebywających na terenie budynku Urzędu Gminy,
2. niewłaściwe parametry środowiska zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego),
3. awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych i informacji, niewłaściwe działanie serwisantów, w tym pozostawienie serwisantów bez nadzoru, a także przyzwolenie na naprawę sprzętu zawierającego dane i informacje poza siedzibą Urzędu Gminy,
4. podejmowanie pracy w systemach z przełamaniem ustalonych zasad lub zaniechaniem stosowania procedur ochrony danych i informacji(praca osoby, która nie jest upoważniona do przetwarzania, próby stosowania nie swojego hasła i identyfikatora przez osoby upoważnione),
5. celowe lub przypadkowe rozproszenie danych i informacji w Internecie z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów systemu informatycznego Urzędu Gminy,
6. ataki z Internetu,
7. naruszenia zasad i procedur określonych w dokumentacji z zakresu ochrony danych i informacji, w tym danych osobowych, przez osoby upoważnione do ich przetwarzania, związane z nieprzestrzeganiem procedur ochrony, w tym zwłaszcza:
   1) niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlania treści danych i informacji na ekranie komputera przed czasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych do zamykanych na klucz szaf dokumentów i wydruków zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu, nieoddanie klucza na portiernię),
   2) naruszenie bezpieczeństwa danych i informacji przez nieautoryzowane ich przetwarzanie,
   3) ujawnienie osobom nieupoważnionym procedur ochrony danych i informacji stosowanych w Urzędzie Gminy,
   4) ujawnienie osobom nieupoważnionym danych i informacji przetwarzanych w Urzędzie Gminy, w tym także nieumyślne ich ujawnienie osobom postronnym, przebywającym bez nadzoru lub niedostatecznie nadzorowanym w pomieszczeniach Urzędu Gminy,
   5) niewykonywanie stosownych kopii zapasowych,
   6) przetwarzanie informacji i danych osobowych w celach prywatnych,
   7) wprowadzanie zmian do systemu informatycznego Urzędu Gminy oraz instalowanie programów bez zgody **Administratora Systemu Informatycznego**.

I. Postanowienia ogólne

1. 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 2002 r. Nr 101, poz. 926 z późn. zm.),(Dz. U. z 2016 roku 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 Podinspektora ds. informatyki, działalności gospodarczej i promocji 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, cyfr 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.

2. **Cel**

Wdrożenie Polityki Bezpieczeństwa w Urzędzie Gminy Mała Wieś ma na celu zabezpieczenie przetwarzanych danych i informacji, w tym przetwarzanych w systemach informatycznych oraz poza nimi, poprzez wykonanie obowiązków wynikających z ustawy i rozporządzenia.
Systemy przetwarzania informacji służą do wspomagania działań Urzędu Gminy Mała Wieś w obszarze obsługi interesantów oraz jego funkcjonowania. Niniejsza polityka ustala sposób ochrony danych i informacji, zbiór zasad i procedur ich przetwarzania w tych systemach oraz prawa, obowiązki i odpowiedzialność osób upoważnionych do dostępu do nich.
W szczególności w systemach przetwarzane są informacje stanowiące dane osobowe w rozumieniu art. 6 ustawy o ochronie danych osobowych. Dane przetwarzane w systemach stanowią informacje niejawne w rozumieniu ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz.U. z 2010 roku, Nr 182, poz. 1228) lub informacje chronione ze względu na ważny interes Urzędu Gminy Mała Wieś.
W związku z tym, że w systemach przetwarzania znajdują się między innymi dane wrażliwe, a system informatyczny posiada szerokopasmowe połączenie z Internetem, zasady i procedury przetwarzania określone w Polityce Bezpieczeństwa służą zapewnieniu wysokiego poziomu bezpieczeństwa.
Osobą odpowiedzialną za bezpieczeństwo informacji chronionych w Urzędzie Gminy Mała Wieś, w tym za ochronę oraz właściwy i niezakłócony przebieg przetwarzania danych w systemach przetwarzania, jest Administrator Bezpieczeństwa Informacji.

3. **Zakres stosowania**

Polityka Bezpieczeństwa dotyczy danych i informacji przetwarzanych w systemie tradycyjnym jak i w systemie informatycznym.
Zasady i procedury określone w Polityce Bezpieczeństwa stosuje się do wszystkich użytkowników informacji oraz innych osób mogących mieć dostęp do danych i informacji lub obszarów i pomieszczeń ich przetwarzania.

II. Organizacja przetwarzania danych

W celu zapewnienia bezpieczeństwa oraz ochrony danych i informacji przetwarzanych w Urzędzie Gminy Mała Wieś ustala się strukturę ochrony danych i informacji, w tym danych osobowych, którą przedstawiono w **załączniku nr 1** do Polityki Bezpieczeństwa.

1. **Administrator Danych** realizuje zadania w zakresie:
   1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych i informacji z uwzględnieniem zmian w obowiązującym prawie, organizacji Urzędu Gminy oraz technikach zabezpieczenia danych i informacji, w tym danych osobowych,
   2) upoważnia osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie odpowiadającym zakresowi ich obowiązków, wykonywanych zadań lub czynności,
   3) wyznacza **Administratora Bezpieczeństwa Informacji** oraz określa zakresu jego zadań i obowiązków,
   4) wskazuje **Administratora Systemów Informatycznych** oraz określa zakresu jego zadań i obowiązków,

5) podejmuje decyzje i działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych i informacji oraz procedur bezpiecznego ich przetwarzania.
6) zgłasza zbiory danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

2. **Administrator Bezpieczeństwa Informacji** nadzoruje przestrzeganie zasad bezpieczeństwa, w tym ochronę oraz właściwy i niezakłócony przebieg przetwarzania danych i informacji w systemach przetwarzania oraz realizuje zadania:
   1) przygotowuje Politykę Bezpieczeństwa i ją aktualizuje,
   2) przygotowuje Instrukcję Zarządzania Systemem Informatycznym i ją aktualizuje,
   3) wnioskuje do Administratora Danych o wskazanie **Administratora Systemu Informatycznego**,
   4) nadzoruje wdrożenie i stosowanie środków fizycznych, organizacyjnych i technicznych w celu zapewnienia bezpieczeństwa danych i informacji przed nieautoryzowanym dostępem, kradzieżą, modyfikacją, zatajeniem bądź utratą,
   5) zatwierdza procedury i regulaminy dotyczące ochrony danych i informacji,
   6) zatwierdza wykaz informacji chronionych,
   7) akceptuje proponowane zmiany oraz modyfikacje procedur i regulaminów,
   8) dokonuje okresowych kontroli przestrzegania przepisów o ochronie danych osobowych,
   9) nadzoruje, pod względem bezpieczeństwa, pracę **Administratorów Informacji** oraz **Administratora Systemu Informatycznego**,
   10) identyfikuje informacje chronione wynikające z przepisów prawa,
   11) zatwierdza Imienne Dokumenty Uprawnień, przygotowywane przez Administratorów Informacji, dotyczące przyznania, modyfikacji lub cofnięcia uprawnień do dostępu do danych i informacji,
   12) przygotowuje imienne upoważnienia przyznania, modyfikacji lub cofnięcia uprawnień do przetwarzania danych, zgodnie z Imiennym Dokumentem Uprawnień, do podpisu przez Administratora Danych,
   13) prowadzi ewidencję osób upoważnionych do przetwarzania danych,
   14) przygotowuje i prowadzi szkolenia z zakresu ochrony danych i informacji osób dopuszczonych do ich przetwarzania,
   15) nadzoruje przygotowanie wniosków zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych,
   16) prowadzi korespondencję z Biurem Generalnego Inspektora Ochrony Danych Osobowych,
   17) nadzoruje przygotowanie umów o powierzenie przetwarzania danych osobowych oraz ich zawieranie,
   18) nadzoruje prawidłowe udostępnianie danych i informacji odbiorcom danych i innym podmiotom,
   19) analizuje raporty wszelkich zdarzeń związanych z bezpieczeństwem informacji ochronionych otrzymywanych od **Administratora Systemu Informatycznego** oraz **użytkowników Informacji**,
   20) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia zasad ochrony i procedur bezpieczeństwa danych i informacji,
   21) informuje Administratora Danych o naruszeniach bezpieczeństwa danych i informacji oraz procedur związanych z bezpiecznym ich przetwarzaniem,
   22) przygotowuje, w porozumieniu z **Administratorem Systemu Informatycznego**, wnioski i propozycje zapotrzebowania na środki finansowe związane z doskonaleniem metod zabezpieczenia technicznego systemów ochrony informacji,

3. **Administrator Systemu Informatycznego** wykonuje zadania w zakresie zarządzania i nadzoru nad funkcjonowaniem systemu informatycznego w Urzędzie Gminy Mała Wieś, a zwłaszcza:

1) zarządza systemem informatycznym, w którym przetwarzane są dane i informacje, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji **Administratora Systemu Informatycznego**,
2) podejmuje działania mające na celu niezawodne zasilanie stacji roboczych i innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych i informacji oraz zagwarantowanie bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji,
3) zapewnia ciągłość działania administrowanych systemów, poprawia ich wydajność oraz instaluje sprzęt i oprogramowanie,
4) udostępnia zasoby informatyczne użytkownikom informacji,
5) decyduje o instalacji nowych elementów w systemach oraz konfiguruje sprzęt i oprogramowanie,
6) nadzoruje działanie ochrony antywirusowej systemie informatycznym,
7) nadzoruje terminowe przeprowadzanie przeglądów i konserwacji sprzętu oraz ich prawidłowy przebieg,
8) nadzoruje prawidłowe przeprowadzania przeglądów programów i narzędzi programowych systemów,
9) nadzoruje wykonywanie napraw urządzeń, dysków i innych elektronicznych nośników informacji, ich konserwację oraz likwidację,
10) opracowuje oraz dokonuje modyfikacji procedur i regulaminów,
11) przydziela odpowiednie prawa dostępu do danych i informacji w określonym systemie oraz określa uprawnienia dla poszczególnych uczestników struktury ochrony informacji,
12) nadaje użytkownikom informacji identyfikatory i hasła dostępu do systemu informatycznego oraz dokonuje ich zmiany,
13) modyfikuje uprawnienia, blokuje i usuwa konta oraz wyrejestrowuje użytkowników informacji zgodnie z zasadami określonymi w Instrukcji Zarządzania Systemem Informatycznym,
14) nadzoruje uwierzytelnianie w systemie użytkowników informacji oraz monitoruje dostęp,
15) prowadzi rejestr zmian haseł użytkowników systemu/programów,
16) prowadzi rejestru oprogramowania udostępnionego użytkownikom,
17) prowadzi rejestr kopii zapasowych,
18) prowadzi rejestr osób dopuszczonych do systemu,
19) określa cykle oraz nośniki archiwizowania danych,
20) nadzoruje wykonywanie kopii zapasowych, ich przechowywanie, weryfikowanie poprawności oraz okresowe sprawdzanie pod kątem dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
21) przeciwdziała dostępowi osób nieupoważnionych do systemu informatycznego,
22) monitoruje na bieżąco błędy systemu oraz przegląda rejestry zdarzeń systemowych,
23) przygotowuje procedury kryzysowe związane z incydentami bezpieczeństwa w systemie informatycznym,
24) prowadzi dokumentację naruszeń bezpieczeństwa danych i informacji w systemie informatycznym,
25) informuje Administratora Bezpieczeństwa Informacji w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego oraz współdziała z nim przy usuwaniu skutków naruszenia,
26) wnioskuje o zatwierdzenie wykazu informacji chronionych,
27) przygotowuje propozycje zapotrzebowania na środki finansowe, związane z doskonaleniem metod zabezpieczenia systemu informatycznego.

4. **Administrator Informacji** decyduje o narzędziach, metodach, miejscu i czasie przetwarzania, przechowywania, tworzenia i niszczenia informacji chronionych w komórce organizacyjnej. Wykonując swoje obowiązki realizuje zadania w zakresie:
   1) przeciwdziałania dostępowi osób nieupoważnionych do systemów przetwarzania,

w których przetwarzane są dane i informacje,
2) nadzoru i kontroli nad zabezpieczeniem danych i informacji, w tym danych osobowych, przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem,
3) kontrolowania dostępu do danych i informacji,
4) nadzoru i kontroli nad udostępnianiem danych i informacji,
5) dokonywania kwalifikacji informacji jako chronionych oraz pisemne zobowiązywanie użytkowników informacji do ich kopiowania w sposób określony przez **Administratora Systemu Informatycznego,**
6) dokonywania oceny przechowywanych danych i informacji pod kątem dalszej ich przydatności dla obsługi interesantów i funkcjonowania Urzędu Gminy Mała Wieś,
7) decydowania o przechowywaniu oraz niszczeniu wydruków zawierających dane i informacje istotne dla obsługi interesantów i funkcjonowaniu Urzędu Gminy Mała Wieś,
8) decydowania o usunięciu przechowywanych danych i informacji,
9) decydowania o przetwarzaniu danych i informacji w zbiorach doraźnych oraz o ich usunięciu,
10) dopuszczania do przetwarzania danych i informacji pracowników oraz nadawania im praw dostępu w określonym systemie,
11) występowania o przydzielenie uprawnień do przetwarzania danych osobom, które w związku z wykonywanymi obowiązkami lub realizowanymi zadaniami będą miały dostęp do danych i informacji chronionych,
12) przygotowywania Imiennego Dokumentu Uprawnień dotyczącego przyznania, modyfikacji lub odebrania upoważnienia do dostępu do informacji chronionych,
13) przygotowywania dla osób upoważnionych do przetwarzania danych aneksów do indywidualnych zakresów czynności,
14) przyjmowania od użytkowników informacji oświadczeń o zachowaniu poufności oraz zachowania tajemnicy,
15) ścisłego współdziałania z **Administratorem Bezpieczeństwa Informacji** w zakresie bezpieczeństwa danych i informacji przetwarzanych w komórkach organizacyjnych,
16) ścisłego współdziałania z **Administratorem Systemu Informatycznego** w zakresie zapewnienia ciągłości funkcjonowania systemu informatycznego w komórkach organizacyjnych,
17) nadzoru i kontroli nad przestrzeganiem przez użytkowników informacji regulaminów i procedur postępowania w zakresie zapewnienia bezpieczeństwa danych i informacji,
18) współdziałania z **Administratorem Bezpieczeństwa Informacji** w zakresie przygotowania wniosków zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych osobowych przetwarzanych w komórkach organizacyjnych.

5. **Użytkownik Informacji** upoważniony do przetwarzania danych i informacji wykonuje zadania w zakresie właściwego i zgodnego z prawem ich przetwarzania, a zwłaszcza:
   1) przetwarza dane wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych w imiennym upoważnieniu i tylko w celu wykonywania nałożonych obowiązków lub wykonania zadań. Zakres dostępu do danych w systemie informatycznym przypisany jest do identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy. Odebranie imiennego upoważnienia do przetwarzania danych powoduje odebranie identyfikatora, wygaśnięcie uprawnień i prawa dostępu do systemu oraz likwidację konta użytkownika,
   2) zachowuje w tajemnicy dane oraz przestrzega procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy oraz sposobów zabezpieczenia danych obowiązuje przez cały okres ważności upoważnienia, po jego odwołaniu, a także po ustaniu zatrudnienia,
   3) zna i stosuje przepisy prawa w zakresie ochrony danych osobowych oraz postanowienia Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym obowiązujących w Urzędzie Gminy Mała Wieś,

4) stosuje określone procedury i regulaminy dotyczące prawidłowego przetwarzania danych oraz zasad ich ochrony,
5) korzysta z systemu informatycznego oraz udostępnionego oprogramowania wyłącznie w celu wykonywania obowiązków służbowych, w sposób zgodny z zaleceniami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników informacji,
6) zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym,
7) podpisuje oświadczenie dotyczące przestrzegania i zachowania poufności oraz zachowania tajemnicy,
8) podpisuje aneks do indywidualnego zakresu czynności,
9) uczestniczy w okresowych szkoleniach dotyczących zasad ochrony danych,
10) uwierzytelnia się w systemie zgodnie z przyznanym upoważnieniem,
11) bezwzględnie przestrzega procedur rozpoczęcia, zawieszenia i zakończenia pracy w systemie,
12) wykonuje kopie zapasowe danych, zgodnie z pisemnym zobowiązywaniem, w sposób określony przez **Administratora Systemu Informatycznego**,
13) przechowuje wymienne, elektroniczne, nośniki informacji w sposób uniemożliwiający nieautoryzowany dostęp do nich,
14) przechowuje dokumentację papierową przetwarzanych danych zgodnie z zasadami określonymi w Polityce Bezpieczeństwa,
15) przechowuje wydruki zawierających dane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych,
16) udostępnia dane zgodnie z decyzją **Administratora Danych,**
17) niszczy (anonimizuje) dane zgodnie z decyzją **Administratora Danych,**
18) niszczy wydruki zgodnie z decyzją **Administratora Danych,**
19) informuje **Administratora Systemu Informatycznego**, o każdej sytuacji odbiegającej od normy w informatycznym systemie przetwarzania,
20) informuje **Administratora Bezpieczeństwa Informacji,** o każdej sytuacji odbiegającej od normy w tradycyjnym systemie przetwarzania,
21) w możliwie pełen sposób dokumentuje stwierdzone zdarzenie mogące mieć wpływ na bezpieczeństwo danych,
22) zgłasza **Administratorowi Systemu Informatycznego** potrzebę przeprowadzenia konserwacji oprogramowania,
23) powstrzymuje się przed dokonywaniem jakichkolwiek zmian w konfiguracji sprzętowej urządzeń.

6. Osoby zobowiązane do zabezpieczenia danych i informacji

Do zabezpieczenia danych i informacji przetwarzanych w Urzędzie Gminy Mała Wieś zobowiązane są osoby sprzątające pomieszczenia oraz inne osoby, które posiadają upoważnienia Administratora Danych do dostępu do obszarów i pomieszczeń przetwarzania danych i informacji. Do ich obowiązków należy:

1) nieujawnianie osobom postronnym procedur i sposobów zabezpieczenia i ochrony danych i informacji stosowanych w Urzędzie Gminy Mała Wieś,
2) nieujawnianie osobom postronnym danych i informacji, do których uzyskały dostęp podczas wykonywania obowiązków służbowych,
3) zabezpieczenie pozostawionych (nieschowanych) po zakończonym dniu pracy wszelkich akt, dokumentów, wydruków oraz nośników elektronicznych mogących zawierać dane i informacje,
4) uczestniczenie w okresowych szkoleniach dotyczących zabezpieczenia danych i informacji,
5) podpisanie oświadczenia dotyczącego przestrzegania i zachowania w tajemnicy sposobów zabezpieczenia przed nieuprawnionym dostępem do danych i informacji, do których uzyskały dostęp podczas wykonywania obowiązków służbowych. Zachowanie

w tajemnicy sposobów zabezpieczenia oraz danych i informacji obowiązuje przez cały okres ważności upoważnienia, po jego odwołaniu, a także po ustaniu zatrudnienia,
6) udokumentowanie, w możliwie pełen sposób, stwierdzonego zdarzenia mogącego mieć wpływ na zabezpieczenie danych i informacji,
7) powiadomienie **Administratora Bezpieczeństwa Informacji** o stwierdzeniu naruszenia bezpieczeństwa danych i informacji,
8) sporządzenie informacji zawierającej datę i godzinę, imię i nazwisko osoby powiadamiającej o zaistniałym zdarzeniu, lokalizację zdarzenia oraz rodzaj naruszenia bezpieczeństwa,
9) bezzwłoczne informowanie **Administratora Bezpieczeństwa Informacji**, o każdej sytuacji odbiegającej od normy mogącej mieć wpływ na bezpieczeństwo danych i informacji.

III. Infrastruktura przetwarzania danych osobowych

1. Obszar ochrony przetwarzania danych i informacji

1) Obszarem chronionym, w którym przetwarzane są dane i informacje jest budynek Urzędu Gminy Mała Wieś, w tym pomieszczenie archiwum, zlokalizowane przy ulicy Jana Kochanowskiego 1.
2) Pomieszczenia chronione przetwarzanych danych i informacji w Urzędzie Gminy Mała Wieś stanowią pokoje określone w załączniku **nr 2** do Polityki Bezpieczeństwa.
3) Kopie zapasowe informacji oraz zbiorów danych przetwarzanych w systemie informatycznym przechowywane są w pomieszczeniu, które stanowi obszar bezpieczny. Dostęp do pomieszczenia posiada **Administrator Systemu Informatycznego** oraz **Administrator Bezpieczeństwa Informacji.**
4) Dane przetwarzane w systemie tradycyjnym przechowywane są w pokojach stanowiących pomieszczenia chronione przetwarzanych danych

2. Zbiory danych przetwarzane w systemach tradycyjnych i informatycznych

1) W systemach przetwarzania zbierane są dane zawierające informacje o interesantach oraz funkcjonowaniu Urzędu Gminy Mała Wieś.
2) Wykaz przetwarzanych zbiorów danych i informacji oraz systemu informatycznego funkcjonujących w Urzędzie Gminy Mała Wieś stanowi załącznik **nr 3** do Polityki Bezpieczeństwa.
3) Procedury oraz sposób zarządzania systemem informatycznym wykorzystywanym przy przetwarzaniu danych określa Instrukcja Zarządzania Systemem Informatycznym.

IV. Struktura zbiorów przetwarzanych w systemach

Opis struktury zbiorów przetwarzanych w systemach informatycznych stanowi załącznik **nr 4** do Polityki Bezpieczeństwa.

V. Przepływ danych pomiędzy poszczególnymi systemami eksploatowanymi w Urzędzie Gminy Mała Wieś

1. Poszczególne systemy/programy informatyczne funkcjonujące w Urzędzie Gminy Mała Wieś nie są ze sobą powiązane. Dane z poszczególnych systemów/programów nie zasilają się wzajemnie.
2. W przyszłości **Administrator Danych** dopuszcza przepływ danych pomiędzy systemami/programami. W takim przypadku **Administrator Bezpieczeństwa Informacji** dokona odpowiednich zmian w zapisach Polityki Bezpieczeństwa wynikających z w/w warunków.
3. Dane przetwarzane w systemach przetwarzania stanowią dane osobowe w rozumieniu ustawy o ochronie danych osobowych.
4. Dane przetwarzane w systemach przetwarzania stanowią informacje niejawne lub chronione ze względu na ważny interes Urzędu Gminy Mała Wieś.

VI. Strategia zabezpieczenia danych oraz środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności danych i informacji przetwarzanych w systemach funkcjonujących w Urzędzie Gminy Mała Wieś

1. Bezpieczeństwo osobowe

1) **Administrator Danych** prowadzi nabór na stanowiska urzędnicze w drodze konkursu. Kandydaci na pracowników są dobierani z uwzględnieniem kompetencji merytorycznych, a także kwalifikacji moralnych. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.
2) Zagrożenie bezpieczeństwa przetwarzanych danych mogące pojawić się ze strony osób, które mają do nich dostęp, jest minimalizowane przez zobowiązywanie do zachowania tajemnicy na podstawie pisemnych oświadczeń.
3) Zagrożenie bezpieczeństwa przetwarzanych danych pojawiające się ze strony osób, które w związku z wykonywanymi czynnościami lub zadaniami mogą uzyskać dostęp do danych (osoby dokonujące napraw, itp.) jest minimalizowane przez zobowiązywanie do zachowania tajemnicy na podstawie pisemnych oświadczeń.
4) Każdy użytkownik informacji przed przystąpieniem do przetwarzania danych obowiązany jest zapoznać się z:
   a) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z późn. zm.), jeżeli wykonywane obowiązki służbowe są związane z danymi osobowymi,
   b) 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),
   c) Podstawowymi zagrożeniami związanymi z przetwarzaniem danych oraz zastosowanymi środkami technicznymi i organizacyjnymi w celu ich ochrony.
5) Każda osoba dopuszczona do przetwarzania danych posiada pisemne upoważnienie Administratora Danych do przetwarzania. W procesie przyznawania upoważnień do przetwarzania danych uczestniczą Administrator Danych, Administrator Bezpieczeństwa Informacji, Administrator Systemu Informatycznego oraz Administratorzy Informacji:
   a) **Administrator Danych** podejmuje decyzje o dopuszczeniu do przetwarzania danych osób, które w związku z obowiązkami służbowymi, zadaniami lub wykonywanymi czynnościami będą miały dostęp do danych i informacji oraz podpisuje dokumenty upoważnień dla osób, które mają zostać dopuszczone do przetwarzania danych.
   b) **Administrator Bezpieczeństwa Informacji** prowadzi ewidencję osób upoważnionych do przetwarzania danych, dokonuje wpisów i aktualizacji w ewidencji oraz przygotowuje upoważnienia do przetwarzania danych.
   c) **Administrator Systemów Informatycznych** nadaje użytkownikowi identyfikator i hasło, rejestruje użytkownika w systemie informatycznym oraz przyznaje określone uprawnienia.
   d) **Administratorzy Informacji** podejmują decyzje o dopuszczeniu do przetwarzania danych osób, które w związku z obowiązkami służbowymi, zadaniami lub wykonywanymi czynnościami będą miały dostęp do danych i informacji, przygotowują Imienne Dokumenty Uprawnień oraz sporządzają aneksy do zakresu obowiązków.
6) Każdej osobie dopuszczonej do dostępu do obszarów i pomieszczeń przetwarzania danych Administrator Danych wydaje pisemne upoważnienie oraz aneks do zakresu obowiązków.

Szczegółową procedurę nadania uprawnień do przetwarzania danych w systemie informatycznych określono w Instrukcji Zarządzania Systemem Informatycznym
Procedurę nadania uprawnień do przetwarzania danych w systemie informatycznym należy stosować odpowiednio w przypadku nadania, modyfikacji lub odebrania uprawnień do przetwarzania danych w systemie tradycyjnym

2. Strefy bezpieczeństwa

1) W Urzędzie Gminy wydzielono strefę bezpieczeństwa klasy I, w której dostęp do danych i informacji zabezpieczony jest wewnętrznymi środkami kontroli. W skład strefy wchodzą:
   a) gabinet Wójta Gminy, w którym może przebywać Wójt Gminy Mała Wieś. Inni upoważnieni użytkownicy informacji oraz osoby postronne mogą przebywać w pomieszczeniu tylko w jego obecności. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
   b) gabinet Zastępcy Wójta - Sekretarza Gminy, w którym może przebywać Zastępca Wójta - Sekretarz Gminy Mała Wieś. Inni upoważnieni użytkownicy informacji oraz osoby postronne mogą przebywać w pomieszczeniu tylko w jego obecności. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
   c) pokój Skarbnika Gminy, w którym może przebywać Skarbnik Gminy Mała Wieś. Inni upoważnieni użytkownicy informacji mogą przebywać w pomieszczeniu tylko w jego obecności. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
   d) pokój Zastępcy Skarbnika Gminy – Głównego Księgowego, w którym może przebywać Zastępca Skarbnika Gminy – Głównego Księgowego Gminy Mała Wieś. Inni upoważnieni użytkownicy informacji mogą przebywać w pomieszczeniu w jego obecności. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
   e) pomieszczenie administracyjne samodzielnego stanowiska ds. zarządzania kryzysowego, obrony cywilnej i spraw obronnych, pełnomocnika ochrony informacji niejawnych, administratora bezpieczeństwa informacji, ochrony danych osobowych, w którym może przebywać Administrator Bezpieczeństwa Informacji. Inni upoważnieni użytkownicy informacji oraz osoby postronne mogą przebywać w pomieszczeniu tylko w jego obecności. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
   f) pomieszczenie administracyjne samodzielnego stanowiska ds. informatyki, promocji gminy, działalności gospodarczej, administratora systemów informatycznych, w którym może przebywać Administrator Systemu Informatycznego. Inni upoważnieni użytkownicy informacji oraz osoby postronne mogą przebywać w pomieszczeniu tylko w jego obecności. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
   g) pomieszczenie administracyjne, w którym przechowywane są kopie zapasowe danych przetwarzanych w systemie informatycznym, w którym mogą przebywać wyłącznie Administrator Systemu Informatycznego oraz Administrator Bezpieczeństwa Informacji. Inni upoważnieni użytkownicy informacji mogą przebywać w pomieszczeniu tylko w ich towarzystwie. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
   h) pomieszczenie administracyjne, w którym upoważnieni użytkownicy informacji oraz osoby postronne mogą przebywać tylko w obecności pracowników referatu Budżetu i Finansów. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
   i) pomieszczenie administracyjne samodzielnego stanowiska ds. kancelaryjnych i organizacyjnych, promocji gminy, obsługi Biuletynu Informacji Publicznej, w którym może przebywać upoważniony użytkownik informacji. Osoby postronne oraz inni użytkownicy informacji mogą przebywać w pomieszczeniu tylko w obecności upoważnionego użytkownika informacji. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.

i) pomieszczenie administracyjne samodzielnego stanowiska ds. kancelaryjnych i organizacyjnych, promocji gminy, obsługi Biuletynu Informacji Publicznej, w którym może przebywać upoważniony użytkownik informacji. Osoby postronne oraz inni użytkownicy informacji mogą przebywać w pomieszczeniu tylko w obecności upoważnionego użytkownika informacji. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
j) pomieszczenia administracyjne, Kierownika Urzędu Stanu Cywilnego, samodzielnego stanowisko ds. wyborów, referendów, wydawania dowodów osobistych, w którym upoważnieni użytkownicy informacji oraz osoby postronne mogą przebywać tylko w obecności Kierownika Urzędu Stanu Cywilnego. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
k) pomieszczenie administracyjne samodzielnego stanowiska ds. realizacji i rozliczania inwestycji, pozyskiwania środków pozabudżetowych, pełnomocnika systemu zarządzania jakością, w którym może przebywać upoważniony użytkownik informacji. Osoby postronne oraz inni użytkownicy informacji mogą przebywać w pomieszczeniu tylko w obecności upoważnionego użytkownika informacji. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
l) pomieszczenie administracyjne samodzielnego stanowiska ds. rolnictwa, geodezji, gospodarki nieruchomościami, w którym może przebywać upoważniony użytkownik informacji. Osoby postronne oraz inni użytkownicy informacji mogą przebywać w pomieszczeniu tylko w obecności upoważnionego użytkownika informacji. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
m) pomieszczenie administracyjne samodzielnego stanowiska ds. inwestycji, budownictwa, gospodarki mieszkaniowej, w którym może przebywać Koordynator-specjalista. Osoby postronne oraz inni użytkownicy informacji mogą przebywać w pomieszczeniu tylko w obecności upoważnionego użytkownika informacji. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
n) pomieszczenie administracyjne samodzielnego stanowiska ds. zamówień publicznych, rozwoju lokalnego, ochrony przeciwpożarowej, w którym może przebywać upoważniony użytkownik informacji. Osoby postronne oraz inni użytkownicy informacji mogą przebywać w pomieszczeniu tylko w obecności upoważnionego użytkownika informacji. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
o) pomieszczenie administracyjne samodzielnego stanowiska ds. kadrowych i socjalnych, bhp, obsługi techniczno-organizacyjnej rady i jej komisji, w którym może przebywać upoważniony użytkownik informacji. Osoby postronne oraz inni użytkownicy informacji mogą przebywać w pomieszczeniu tylko w obecności upoważnionego użytkownika informacji. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
p) pomieszczenie administracyjne samodzielnego stanowiska ds. ewidencji ludności, kultury, sportu i zdrowia, współpracy z organizacjami pozarządowymi, w którym może przebywać upoważniony użytkownik informacji. Osoby postronne oraz inni użytkownicy informacji mogą przebywać w pomieszczeniu tylko w obecności upoważnionego użytkownika informacji. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
q) pomieszczenie administracyjne samodzielnego stanowiska ds. gospodarki przestrzennej i ochrony środowiska, w którym może przebywać upoważniony użytkownik informacji. Osoby postronne oraz inni użytkownicy informacji mogą przebywać w pomieszczeniu tylko w obecności upoważnionego użytkownika informacji. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
r) pomieszczenie administracyjne samodzielnego stanowiska ds. gospodarki odpadami i ochrony środowiska, komunikacji, zaopatrzenia w energię elektryczną, w którym może przebywać upoważniony użytkownik informacji. Osoby postronne oraz inni

użytkownicy informacji mogą przebywać w pomieszczeniu tylko w obecności upoważnionego użytkownika informacji. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.

s) pomieszczenie administracyjne samodzielnego stanowiska ds. ochrony środowiska, rozliczeń opłat za odpady komunalne, w którym może przebywać upoważniony użytkownik informacji. Osoby postronne oraz inni użytkownicy informacji mogą przebywać w pomieszczeniu tylko w obecności upoważnionego użytkownika informacji. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
t) pomieszczenie administracyjne samodzielnego stanowiska ds. zezwoleń na sprzedaż napojów alkoholowych, w którym może przebywać upoważniony użytkownik informacji. Osoby postronne oraz inni użytkownicy informacji mogą przebywać w pomieszczeniu tylko w obecności upoważnionego użytkownika informacji. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
u) pomieszczenie administracyjne Koordynatora ds. Rozwiązywania Problemów Alkoholowych, w którym może przebywać upoważniony użytkownik informacji. Osoby postronne oraz inni użytkownicy informacji mogą przebywać w pomieszczeniu tylko w obecności upoważnionego użytkownika informacji. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
v) pomieszczenie administracyjne samodzielnego stanowiska ds. dróg i ulic, w którym może przebywać upoważniony użytkownik informacji. Osoby postronne oraz inni użytkownicy informacji mogą przebywać w pomieszczeniu tylko w obecności upoważnionego użytkownika informacji. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
w) pomieszczenie administracyjne, w którym może przebywać Radca Prawny. Inni upoważnieni użytkownicy informacji mogą przebywać w pomieszczeniu tylko w jego obecności. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
x) pomieszczenie archiwum Urzędu Gminy Mała Wieś, w którym mogą przebywać tylko upoważnieni użytkownicy informacji. Klucze do pomieszczenia są przechowywane w miejscu bezpiecznym.
y) pomieszczenie Kancelarii Tajnej, w którym może przebywać wyłącznie Pełnomocnik ds. Ochrony Informacji Niejawnych. Osoby postronne w ogóle nie mają dostępu do pomieszczenia. Złożony na portierni klucz do pomieszczenia jest przechowywany w woreczku zalakowanym referentką.

2) W strefie bezpieczeństwa klasy II do danych i informacji mają dostęp wszystkie osoby upoważnione do przetwarzania, zgodnie z zakresem upoważnienia do ich przetwarzania. Osoby postronne mogą w niej przebywać tylko w obecności pracowników upoważnionych do przetwarzania danych i informacji. Strefa ta obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych i informacji.

3. Zabezpieczenie sprzętu stosowane przez Administratora Danych

1) Serwer jest zlokalizowany w odrębnym, klimatyzowanym pomieszczeniu. Pomieszczenie nie posiada okien.
2) O zasilaniu urządzeń za pośrednictwem zasilaczy awaryjnych (UPS) decyduje **Administrator Systemu Informatycznego.**
3) Okablowanie sieciowe zostało zaprojektowane w sposób umożliwiający dostęp do linii teletransmisyjnych tylko z pomieszczeń zamykanych na klucz. Kable sieciowe nie krzyżują się z okablowaniem zasilającym.
4) Bieżąca konserwacja sprzętu informatycznego wykorzystywanego do przetwarzania danych i informacji wykonywana jest wyłącznie przez **Administratora Systemu Informatycznego**. Poważne naprawy wykonywane przez podmioty zewnętrzne realizowane są w siedzibie Urzędu Gminy Mała Wieś, po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych określającej kary umowne za naruszenie bezpieczeństwa danych.

5) **Administrator Systemu Informatycznego** dopuszcza konserwację i naprawę sprzętu informatycznego poza siedzibą Urzędu Gminy Mała Wieś. W takim przypadku, przed przekazaniem sprzętu, wymontowywane są z niego nośniki informacji zawierające dane i informacje chronione.
6) Zużyty sprzęt służący do przetwarzania może być zbywany dopiero po trwałym usunięciu danych i informacji, a urządzenia uszkodzone mogą być przekazywane do utylizacji właściwym podmiotom, jeśli trwałe usunięcie danych i informacji wymagałoby nadmiernych nakładów, po zawarciu umowy powierzenia przetwarzania danych.
7) W przypadku uszkodzenia elementu sprzętu informatycznego zawierającego nośnik informacji, na którym zapisane są informacje chronione i dane osobowe, wymagającego przekazania go poza siedzibę Urzędu Gminy Mała Wieś, nośnik jest wymontowywany, a następnie niszczony.
8) Rejestracji podlegają wszystkie przypadki awarii systemu informatycznego, działania konserwacyjne w systemie oraz naprawy systemu. Są one opisywane w stosownych protokołach, podpisywanych przez osoby uczestniczące w tych działaniach, a także **Administratora Bezpieczeństwa Informacji**.
9) Rejestracji podlegają wszystkie przypadki naruszenia bezpieczeństwa danych i informacji oraz procedur związanych z bezpiecznym ich przetwarzaniem stwierdzone w tradycyjnym i informatycznym systemie przetwarzania.
10) **Administrator Systemu Informatycznego** przekazuje użytkownikom informacji zasady dotyczące postępowania mającego na celu zapewnienie prawidłowej eksploatacji systemu informatycznego, a zwłaszcza odnoszące się do:
    a) ochrony elektromagnetycznej nośników danych, a szczególnie nośników danych, na których są przechowywane kopie zapasowe,
    b) prawidłowej lokalizacji komputerów,
    c) właściwej eksploatacji udostępnionego sprzętu informatycznego,
    d) właściwej eksploatacji udostępnionego oprogramowania,
    e) przestrzegania zasad pracy w systemie informatycznym,
    f) wykonywania kopii danych, w tym kopii zapasowych.
11) Duplikaty kluczy do pomieszczeń stanowiących obszar ochrony systemów przetwarzania przechowywane są w metalowych skrzynkach (w zapieczętowanych kopertach). Prawo pobrania kluczy (otwarcia kopert) mają Administrator Danych oraz Administrator Bezpieczeństwa Informacji. Z pobrania duplikatów kluczy sporządzany jest protokół.

4. Zasady zabezpieczeń stosowane przez osoby upoważnione

Każda osoba upoważniona do przetwarzania danych i informacji jest zobowiązana do:
1) zachowania w tajemnicy danych i informacji, w tym także wobec najbliższych,
2) ustawienia monitora komputera w taki sposób, by osoby niepowołane nie mogły widzieć jego zawartości, a zwłaszcza nieustawiania go naprzeciwko wejścia do pomieszczenia,
3) niepozostawiania bez nadzoru i kontroli dokumentów i nośników danych i informacji w miejscach publicznych oraz w samochodach,
4) dbania o zapewnienie prawidłowej wentylacji komputerów (nie zasłaniania kratek wentylatorów meblami, zasłonami lub ustawiania tuż przy ścianie),
5) niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie łatwo powodujących spięcia (grzejniki, czajniki, wentylatory, itp.),
6) należytego pilnowania akt, dyskietek, pamięci przenośnych i komputerów przenośnych,
7) kasowania danych i informacji po ich wykorzystaniu, zgodnie z procedurą, szczególnie na dyskach i pamięciach przenośnych
8) niezapisywania hasła wymaganego do uwierzytelnienia się w systemie w miejscu dostępnym i widocznym,
9) niewprowadzania zmian w oprogramowaniu i konfiguracji powierzonego sprzętu (w tym komputerów przenośnych) nawet, gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych i informacji,

10) przestrzegania swoich uprawnień w systemie, właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń **Administratora Bezpieczeństwa Informacji** oraz **Administratora Systemu Informatycznego**,
11) opuszczania stanowiska pracy dopiero po zablokowaniu stacji roboczej,
12) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane i informacje, bez obecności osoby upoważnionej do przetwarzania,
13) kopiowania tylko jednostkowych danych (pojedynczych plików). Zakazane jest robienie kopii całych zbiorów danych i informacji lub takich ich części, które nie są konieczne do wykonywania obowiązków. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne oraz przechowywane w zamykanych na klucz szafach. Po ustaniu przydatności tych kopii dane i informacje, zgodnie z procedurą, muszą być trwale skasowane lub zniszczone fizycznie nośniki, na których są przechowywane,
14) udostępniania danych i informacji, w tym danych osobowych, zgodnie z procedurą. Dane i informacje przekazywane pocztą elektroniczną mogą być udostępnione wyłącznie po zastosowaniu kryptograficznej ochrony danych i informacji,
15) niepodawania w rozdzielniku pism oraz decyzji informacji o adresach stron.
Zaleca się stosowanie rozdzielników do pism i decyzji z pełną identyfikacją strony, które pozostają w aktach sprawy.
16) niewynoszenia na jakichkolwiek nośnikach całych zbiorów danych i informacji, nawet w postaci zaszyfrowanej,
17) niewynoszenia na jakichkolwiek nośnikach wypisów ze zbiorów danych i informacji, nawet w postaci zaszyfrowanej, bez zgody **Administratora Danych,**
18) wykonywania kopii roboczych przetwarzanych danych i informacji z częstotliwością, która zapobiegnie ich utracie,
19) wykonywania kopii zapasowych przetwarzanych danych i informacji, w sposób określony przez **Administratora Systemu Informatycznego**,
20) zakończenia pracy na stacji roboczej (komputerze przenośnym) po zapisaniu przetwarzanych danych, a następnie prawidłowym wylogowaniu się i wyłączeniu komputera,
21) niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane i informacje przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy,
22) chowania do zamykanych na klucz szaf wszelkich akt zawierających dane i informacje przed opuszczeniem miejsca pracy oraz po zakończeniu dnia pracy,
23) umieszczania, po zakończeniu pracy, kluczy do szaf w ustalonym, miejscu,
24) zamykania okien w razie opadów lub innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych i informacji,
25) zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy,
26) zamknięcia drzwi na klucz po zakończeniu dnia pracy i oddania klucza do przechowania w miejscu bezpiecznym. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów zawierających dane i informacje w zamykanych szafach, należy powiadomić o tym przełożonego, który zgłasza osobie sprzątającej rezygnację z wykonania usługi sprzątania. W takim przypadku także należy zostawić klucz do przechowania w miejscu bezpiecznym.

5. Postępowanie z nośnikami i ich bezpieczeństwo

1) Dane z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemów informatycznych **Administratora Danych** powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale usuwającym pliki.
2) Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy

szerokie wypisy ze zbiorów) lub informacje mogą być przechowywane na specjalnie oznaczonych nośnikach.

3) Nośniki są przechowywane w szafach zamykanych na klucz, niedostępnych dla osób nieupoważnionych. Po ustaniu przydatności danych lub informacji należy je trwale skasować lub zniszczyć nośnik,
4) Uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników, przeciąć lub przełamać,
5) Zabrania się powtórnego używania do sporządzania brudnopisów pism, jednostronnie zadrukowanych kart, jeśli zawierają one dane.
   Zaleca się dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów,
6) Po wykorzystaniu wydruki zawierające dane i informacje należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać wydruków, w czasie dnia pracy, na biurku,
   Wydruków nie wolno wynosić poza siedzibę Urzędu Gminy Mała Wieś.

6. Wymiana danych i ich bezpieczeństwo

1) Bezpieczeństwo danych, a w szczególności ich integralność i dostępność, w dużym stopniu zależy od zdyscyplinowanego, codziennego umieszczania danych w odpowiednich bazach/zbiorach stacji roboczych oraz wyznaczonych zasobach serwera. Pozwala to, uniknąć wielokrotnego wprowadzania tych samych danych do systemu informatycznego.
2) Sporządzanie kopii zapasowych następuje w trybie określonym w Rozdziale VII Instrukcji Zarządzania Systemem Informatycznym.
3) Inne wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi producentów sprzętu i używanych programów, wskazówkach **Administratora Bezpieczeństwa Informacji, Administratora Systemu Informatycznego** oraz Instrukcji Zarządzania Systemem Informatycznym.
4) Pocztą elektroniczną można przesyłać tylko jednostkowe dane i informacje, a nie całe bazy lub szerokie z nich wypisy, po zastosowaniu ochrony kryptograficznej. Procedura ta chroni przesyłane dane przed „przesłuchami" na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w Internecie.
5) Przed atakami z sieci zewnętrznej (Internet) wszystkie komputery **Administratora Danych** (w tym także przenośne) chronione są środkami dobranymi przez **Administratora Systemu Informatycznego,** w porozumieniu z **Administratorem Bezpieczeństwa Informacji**. Użytkownicy zobowiązani są do zwracania uwagi na to, czy urządzenie, na którym pracują, domaga się aktualizacji zabezpieczeń. O wszystkich takich przypadkach użytkownicy zobowiązani są do informowania **Administratora Systemu Informatycznego** oraz umożliwić mu monitorowanie oraz aktualizację środków bezpieczeństwa.
6) **Administrator Systemu Informatycznego** w porozumieniu z **Administratorem Bezpieczeństwa Informacji** dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego i powiększania baz danych. **Administrator Bezpieczeństwa Informacji** oraz **Administrator Systemu Informatycznego** obserwują, czy rozwijający się system zabezpieczeń nie wywołuje nowych zagrożeń.
7) Stosowane sposoby kryptograficznej ochrony danych i informacji:
   a) przesyłanie danych za pomocą poczty elektronicznej – stosuje się POP – tunelowanie, szyfrowanie połączenia, korzystanie z usług antyspamowych, z www Spoofing,
   b) przesyłanie danych pracowników, niezbędne do wykonania przelewów wynagrodzeń - stosuje się wydzielone połączenie internetowe.

7. Udostępnianie danych osobowych

1) Podstawą do udostępnienia danych jest ustawa o ochronie danych osobowych lub ustawy szczególne.
2) Udostępnianie danych osobowych odbiorcom danych może nastąpić wyłącznie na podstawie złożonego wniosku.
   Wniosek ten powinien mieć formę pisemną i zawierać:
   a) dokładne oznaczenie administratora danych,
   b) dokładne oznaczenie wnioskodawcy,
   c) wskazanie przepisów prawa uprawniających do dostępu lub otrzymania informacji,
   d) oznaczenie zbioru, w którym żądane dane się znajdują,
   e) określenie rodzaju, zakresu i przeznaczenia potrzebnych danych oraz formy ich przekazania lub udostępnienia,
   f) wskazanie imienia, nazwiska osoby występującej o udostępnienie danych.
3) Udostępnienie danych osobowych na podstawie ustnego wniosku zawierającego wszystkie elementy wniosku pisemnego może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania w sytuacji wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.
4) Osoba udostępniająca dane osobowe jest obowiązana zażądać pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść danych.
5) W przypadku przekazywania informacji na podstawie wniosku ustnego, należy stosownie do okoliczności, zwrócić się z prośbą o pokwitowanie pobrania lub potwierdzenie odbioru (otrzymania) danych.
6) Fakt udostępnienia danych i informacji należy odnotować w systemie informatycznym bądź w prowadzonej ewidencji udostępniania danych.

8. Kontrola dostępu do systemów

1) Pracownikom Urzędu Gminy Mała Wieś, konta opatrzone identyfikatorem, umożliwiające dostęp do danych i informacji, przydziela się zgodnie z Imiennym Dokumentem Uprawnień. **Administrator Systemu Informatycznego** przydziela pracownikowi konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem.
2) W razie potrzeby, po uzyskaniu akceptacji **Administratora Bezpieczeństwa Informacji**, **Administrator Systemu Informatycznego** może przydzielić konto opatrzone identyfikatorem innej osobie, nieposiadającej statusu pracownika Urzędu Gminy Mała Wieś.
3) Pierwsze hasło wymagane do uwierzytelnienia się w systemie przydziela **Administrator Systemu Informatycznego**, po odebraniu od osoby upoważnionej do przetwarzania danych i informacji oświadczenia zawierającego zobowiązanie do zachowania w tajemnicy pierwszego i następnych haseł oraz potwierdzenie odbioru pierwszego hasła.
4) Zagwarantowanie poufności i integralności danych i informacji wymaga przestrzegania przez użytkowników informacji swoich uprawnień w systemie, właściwego korzystania z baz danych, używania wyłączanie własnego identyfikatora i hasła oraz stosowania się do zaleceń **Administratora Bezpieczeństwa Informacji** i **Administratora Systemu Informatycznego.**
5) Kontrolę przestrzegania, przez użytkowników informacji, zasad o których mowa w pkt. 4 sprawują **Administrator Bezpieczeństwa Informacji** oraz **Administrator Systemu Informatycznego.**

9. Kontrola dostępu do sieci

1) System informatyczny posiada szerokopasmowe połączenie z Internetem. Dostęp do Internetu jest ograniczony. Na poszczególnych stacjach roboczych można przeglądać wyznaczone strony www.

2) **Administrator Danych** wykorzystuje centralną zaporę sieciową w celu separacji lokalnej

sieci od sieci publicznej.

3) Korzystanie z zasobów sieci wewnętrznej (intranet) jest możliwe tylko w zakresie uprawnień przypisanych do danego konta osoby upoważnionej do przetwarzania danych.
4) Operacji za pośrednictwem rachunku bankowego może dokonywać wyłącznie pracownik księgowości upoważniony przez Administratora Danych, po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

10. Komputery przenośne i praca na odległość

1) Urządzenia przenośne oraz nośniki danych wynoszone z siedziby **Administratora Danych** nie powinny być pozostawiane bez nadzoru w miejscach publicznych. Komputery przenośne należy transportować w torbach służbowych. Stosowanie własnych charakterystycznych toreb jest niedopuszczalne.
2) Niedopuszczalne jest pozostawianie bez nadzoru i kontroli sprzętu komputerowego w hotelach, miejscach publicznych oraz w samochodach.
3) Dane i informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu.
4) Wykorzystywanie komputerów przenośnych w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych, stwarza warunki minimalizujące ryzyko zapoznania się z danymi i informacjami przez osoby nieupoważnione. Niedozwolone jest korzystanie z komputera przenośnego w restauracjach czy środkach komunikacji publicznej.
5) Niedozwolone jest udostępnianie domownikom komputera przenośnego należącego do Administratora Danych. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym.
6) Komputery przenośne **Administratora Danych** są powierzane użytkownikom informacji, na podstawie dokumentu powierzenia komputera przenośnego.
7) **Administrator Systemu Informatycznego**, wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym oraz określa zasady:
   a) postępowania w razie nieobecności w pracy dłuższej niż 5 dni. Jeżeli komputer przenośny nie może być zwrócony przed okresem nieobecności, to użytkownik tego komputera powinien niezwłocznie powiadomić o tym **Administratora Bezpieczeństwa Informacji** i uzgodnić z nim zwrot komputera przenośnego Administratorowi Danych,
   b) zwrotu sprzętu w razie zakończenia pracy w Urzędzie Gminy Mała Wieś.
8) W zakresie nieuregulowanym w Polityce Bezpieczeństwa do pracy z wykorzystaniem komputerów przenośnych stosuje się postanowienia Instrukcji Zarządzania Systemem Informatycznym.

11. Monitorowanie dostępu do systemów i ich użycia

1) System zapewnia odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu,
   b) identyfikatora użytkownika wprowadzającego dane do systemu,
   c) źródła danych - w przypadku zbierania danych nie od osoby, której one dotyczą,
   d) informacji o odbiorcach danych, którym dane zostały udostępnione oraz dacie i zakresie tego udostępnienia,
   e) sprzeciwu wobec przetwarzania danych, o którym mowa w art. 32 ust. 1 pkt. 8 ustawy.
2) Odnotowywanie informacji, o których mowa w pkt. a) i b), następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3) Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w pkt. a-e.
4) **Administrator Systemu Informatycznego** przeprowadza synchronizację zegarów stacji roboczych z serwerem, ograniczając dopuszczalność zmian w ustawieniach zegarów,
5) Jakiekolwiek zmiany ustawień zegarów mogą być dokonywane jedynie przez **Administratora Systemu Informatycznego**.
6) System informatyczny **Administratora Danych** umożliwiają zapisywanie zdarzeń na potrzeby audytu i przechowywanie informacji o nich przez określony czas. Zapisy te obejmują:
   a) identyfikator użytkownika,
   b) datę i czas zalogowania i wylogowania się z systemu,
   c) tożsamość stacji roboczej,
   d) zapisy udanych i nieudanych prób dostępu do systemu,
   e) zapisy udanych i nieudanych prób dostępu do danych osobowych i innych zasobów systemowych.

12. Przeglądy okresowe zapobiegające naruszeniom obowiązku szczególnej staranności Administratora Danych

1) **Administrator Bezpieczeństwa Informacji** przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania. Osoby upoważnione do przetwarzania danych są obowiązane do współpracy z **Administratorem Bezpieczeństwa Informacji** oraz wskazywać dane, które powinny zostać usunięte ze względu na zrealizowanie celu przetwarzania danych lub brak ich adekwatności do realizowanego celu.
2) **Administrator Bezpieczeństwa Informacji** może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych. Dodatkowy przegląd jest możliwy także w sytuacji zmian organizacyjnych **Administratora Danych**.
3) Z przebiegu usuwania danych należy sporządzić protokół opracowywany i podpisywany przez użytkownika informacji odpowiedzialnego za przetwarzane dane. Protokół zatwierdza **Administrator Bezpieczeństwa Informacji**.
4) Wzory dokumentów przewidujących powiadomienie, o którym mowa w art. 24 i 25 ustawy, mogą być stosowane po zaakceptowaniu przez **Administratora Bezpieczeństwa Informacji.**
5) Użytkownicy Informacji sporządzają, prowadzą i uaktualniają wykazy przepisów na mocy, których przetwarzają, funkcjonujące u nich, zbiory danych.
6) **Administrator Bezpieczeństwa Informacji** przygotowuje wykaz zbiorów danych, w którym poszczególnym kategoriom danych i informacji przypisane zostały okresy ich przechowywania. Wykaz ten sporządzany jest po przeanalizowaniu przepisów wyznaczających m.in. obowiązek przechowywania dokumentacji czy też okresy przedawnienia roszczeń dokumentowanych z wykorzystaniem danych i informacji.
7) Przed sporządzeniem wykazu, o którym mowa wyżej, należy przygotować wykaz przepisów na mocy, których przetwarzane są dane i informacje, sporządzony na podstawie wykazów cząstkowych przygotowanych przez poszczególne komórki organizacyjne.

13. Szkolenia w zakresie ochrony danych

1) **Administrator Bezpieczeństwa Informacji** przygotowuje i prowadzi szkolenia z zakresu przetwarzania oraz ochrony danych obejmujące:
   a) pracowników, którzy mają zostać upoważnieni do przetwarzania danych,
   b) osoby wykonujące pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, odbywające staż, wolontariuszy, które mają zostać upoważnione do przetwarzania danych,

c) inne osoby, które mają zostać upoważnione do przetwarzania danych lub ich zabezpieczenia, jeżeli z zakresu ich zadań lub działalności wynika konieczność dostępu lub obowiązek ochrony i zabezpieczenia danych,
d) wszystkie osoby wymienione w pkt. a - c, w przypadku każdej zmiany zasad przetwarzania lub procedur ochrony,

2) Tematyka szkoleń obejmuje:
a) zasady i procedury dotyczące ochrony danych, sporządzania i przechowywania kopii, niszczenia wydruków i zapisów na nośnikach informacji,
b) sposoby ochrony danych przed osobami nieupoważnionymi oraz procedury udostępniania danych,
c) obowiązki osób upoważnionych do przetwarzania danych,
d) odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych,
e) Politykę Bezpieczeństwa i Instrukcję Zarządzania Systemem Informatycznym w Urzędzie Gminy Mała Wieś – zasady i procedury przetwarzania oraz ochrony danych.

14. Odpowiedzialność osób upoważnionych do przetwarzania danych

1) Niestosowanie się do obowiązującej Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym oraz naruszenie lub złamanie zasad i procedur ochrony danych przez pracowników upoważnionych do ich przetwarzania może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym na podstawie Kodeksu Pracy.
2) Osoby naruszające zasady i procedury przetwarzania oraz ochrony danych będą pociągnięte do odpowiedzialności karnej, na podstawie art. 51-52 ustawy oraz art. 266-269 Kodeksu Karnego.

15. Zastosowane środki techniczne i organizacyjne

W celu zapewnienia ochrony danych i informacji, w tym zabezpieczenia danych osobowych przed nieupoważnionym dostępem wprowadza się niżej określone rozwiązania techniczne i organizacyjne:

1) Środki ochrony fizycznej

a) Dostęp do obszaru i pomieszczeń przetwarzania danych w Urzędzie Gminy w Małej Wsi, w godzinach pracy, nadzorowany jest przez upoważnionych pracowników.
b) Po godzinach pracy dostęp do budynku jest zabezpieczony systemem alarmowym nadzorowanym przez firmę ochrony osób i mienia.
c) Po godzinach pracy dostęp do obszaru i pomieszczeń przetwarzania danych mają osoby sprzątające pomieszczenia posiadające upoważnienia Administratora Danych do dostępu do tych pomieszczeń.
d) Urządzenia służące do przetwarzania informacji znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi.
e) Dokumenty papierowe przetwarzanych danych przechowywane są w zamykanych szafach biurowych, w pomieszczeniach, gdzie są przetwarzane.
f) Pomieszczenie Kancelarii Tajnej nie posiada okna.
g) Zastosowano zamykane szafy do przechowywania kopii zapasowych i wymiennych nośników danych.
h) Klucze od pomieszczeń, po godzinach pracy, są przechowywane w kasetce metalowej w miejscu bezpiecznym.
i) Kopie zapasowe zbiorów danych są przechowywane w innych pomieszczeniach niż komputery, na których są przetwarzane na bieżąco.

2) Środki sprzętowe, informatyczne i telekomunikacyjne

a) Zastosowano niszczarki dokumentów.
b) Urządzenia wchodzące w skład systemów informatycznych podłączone są do odrębnego obwodu elektrycznego.

c) Zastosowano sieć lokalną w topologii gwiazdy.
d) Dane są przetwarzane w sposób zarówno scentralizowany jak i rozproszony.
e) Sieć lokalna jest podłączona do Internetu.
f) Kopie awaryjne wykonywane są na nośnikach CD i DVD, HDD.

3) **Środki ochrony w ramach oprogramowania urządzeń teletransmisji**
a) Zastosowano programy firewall na komputerach spełniających funkcje bram internetowych.
b) Zastosowano działający w „tle" program antywirusowy na komputerach użytkowników informacji.
c) Zastosowano programy firewall na komputerach użytkowników systemów.
d) Zastosowano hasła dostępu do komputerów i systemów operacyjnych.

4) **Środki ochrony w ramach oprogramowania systemów**
a) Dostęp fizyczny do baz danych zastrzeżony jest wyłącznie dla **Administratora Systemu Informatycznego.**
b) Konfiguracja systemów umożliwia użytkownikom końcowym dostęp do danych i informacji jedynie za pośrednictwem aplikacji.
c) System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.
d) Na komputerach użytkowników działa w „tle" program antywirusowy.

5) **Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych**
a) Automatycznie rejestrowany jest identyfikator użytkownika wprowadzającego dane oraz datę pierwszego wprowadzenia tych danych.
b) Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.
c) Dla każdego użytkownika systemu jest ustalony odrębny identyfikator.
d) Zdefiniowano użytkowników oraz ich prawa dostępu do danych i informacji na poziomie aplikacji.

6) **Środki ochrony w ramach systemu użytkowego**
a) Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.
b) Komputery, z których możliwy jest dostęp do danych osobowych zabezpieczone są hasłami uruchomieniowymi.
c) Zastosowano blokady w przypadku dłuższej nieaktywności użytkownika.

7) **Środki organizacyjne**
a) Powołano **Administratora Bezpieczeństwa Informacji – Kamila Bernackiego** - (tel. 24 2697799).
b) Wyznaczono **Administratora Systemu Informatycznego – Adama Kacprzaka** (tel. 24 2697975).
c) Ustalono Politykę Bezpieczeństwa.
d) Ustalono Instrukcję Zarządzania Systemem Informatycznym.
e) Określono system i procedurę nadawania upoważnień oraz dopuszczania osób do przetwarzania danych osobowych.
f) Do przetwarzania danych dopuszczane są wyłącznie osoby posiadające imienne upoważnienie Administratora Danych, wystawiane na podstawie imiennego dokumentu uprawnień.
g) Prowadzona jest ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych.
h) Osoby upoważnione do przetwarzania danych osobowych, przed dopuszczeniem ich do tych danych, są szkolone w zakresie obwiązujących przepisów o ochronie danych osobowych, zasad i procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemach funkcjonujących w Urzędzie Gminy Mała Wieś.

i) Osoby inne niż użytkownicy informacji, posiadają upoważnienia Administratora Danych do dostępu do obszaru i pomieszczeń przetwarzania danych.
j) Osoby posiadające upoważnienia do dostępu do obszaru i pomieszczeń przetwarzania danych składają pisemne oświadczenia o zachowaniu w tajemnicy sposobów zabezpieczenia przed nieuprawnionym dostępem oraz o zachowaniu w tajemnicy danych, do których uzyskały dostęp podczas wykonywania obowiązków służbowych.
k) Osoby posiadające upoważnienia do dostępu do obszaru i pomieszczeń przetwarzania danych są szkolone przez Administratora Bezpieczeństwa Informacji w zakresie obwiązujących przepisów o ochronie danych osobowych, w tym Polityki Bezpieczeństwa, zasad i procedur zabezpieczenia danych oraz informowane o podstawowych zagrożeniach związanych z bezpieczeństwem danych przetwarzanych w systemach funkcjonujących w Urzędzie Gminy Mała Wieś.
l) Ustalono indywidualne zakresy czynności dla osób zatrudnionych przy przetwarzaniu danych osobowych oraz odpowiedzialności za ochronę tych danych.
m) Ustalono aneksy do indywidualnych zakresów czynności dla osób zobowiązanych do zabezpieczenia danych.
n) Osoby zatrudnione przy przetwarzaniu informacji, w tym danych osobowych, zobowiązane są do zachowania ich w tajemnicy.
o) Wydruki zawierające dane osobowe nie są wykonywane na drukarce sieciowej.
p) Korespondencja z interesantami jest prowadzona pocztą priorytetową (listy polecone).
q) Imienny Dokument Uprawnień jest podstawą do wydania imiennego upoważnienia do przetwarzania danych osobowych.
r) Korespondencja z interesantami jest prowadzona pocztą priorytetową (listy polecone).
s) Zdefiniowano procedury postępowania w sytuacji:
   - naruszenia ochrony danych,
   - słabości systemu informatycznego,
   - niewłaściwego funkcjonowania oprogramowania.
t) W przypadku przetwarzania dokumentacji papierowej stosuje się odpowiednio procedury dotyczące przetwarzania w systemie informatycznym.

VII. Przeglądy polityki bezpieczeństwa i audyty systemów

1. Polityka Bezpieczeństwa powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych i informacji **Administrator Bezpieczeństwa Informacji** może wcześniej dokonać przeglądu Polityki Bezpieczeństwa Informacji.
2. **Administrator Bezpieczeństwa Informacji** analizuje, czy Polityka Bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych i informacji jest adekwatna do:
   1) zmian w budowie systemu informatycznego,
   2) zmian organizacyjnych w Urzędzie Gminy Mała Wieś, w tym również zmian statusu osób upoważnionych do przetwarzania danych i informacji,
   3) zmian w obowiązującym prawie.
3. **Administrator Bezpieczeństwa Informacji** po uzgodnieniu z **Administratorem Danych** może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z **Administratorem Systemu Informatycznego**. Zakres, przebieg i wyniki audytu dokumentowane są w protokole podpisywanym przez **Administratora Bezpieczeństwa Informacji** oraz **Administratora Systemu Informatycznego**.
4. **Administrator Danych**, biorąc pod uwagę wnioski **Administratora Bezpieczeństwa Informacji**, może zlecić przeprowadzenie audytu przez wyspecjalizowany podmiot zewnętrzny.

VIII. Postanowienia końcowe

1. Każda osoba upoważniona do przetwarzania danych i informacji zobowiązana jest do zapoznania się z przepisami prawa dotyczącymi przetwarzania oraz ochrony danych osobowych.
2. Każda osoba upoważniona do przetwarzania danych i informacji zobowiązana jest do zapoznania się, przed dopuszczeniem do przetwarzania, z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.
3. Przy przetwarzaniu danych i informacji oraz ochrony w systemie tradycyjnym (papierowym), o ile nie określono tego odrębnie, stosuje się odpowiednie procedury dotyczące przetwarzania i ochrony w systemie informatycznym.
4. W przypadku naruszenia zasad bezpieczeństwa danych i informacji przetwarzanych w systemie tradycyjnym stosuje się odpowiednio procedurę naruszenia zasad bezpieczeństwa przetwarzania danych i informacji w systemie informatycznym określoną w Instrukcji Zarządzania Systemem Informatycznym.

Dokument powiązany: ***Instrukcja Zarządzania Systemem Informatycznym w Urzędzie Gminy Mała Wieś.***

Administrator

Bezpieczeństwa Informacji