Zarządzenie Nr 159/2008
Wójta Gminy Brudzeń Duży
z dnia 10 grudnia 2008 roku

w sprawie Polityki Bezpieczeństwa w Urzędzie Gminy w Brudzeniu Dużym

Na podstawie § 3 i 4 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 r. Nr 100, poz. 1024) zarządza się co następuje:

§ 1

Wprowadza się Politykę Bezpieczeństwa w Urzędzie Gminy w Brudzeniu Dużym stanowiącą załącznik do niniejszego zarządzenia.

§ 2

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji w Urzędzie Gminy w Brudzeniu Dużym.

§ 3

Traci moc Zarządzenia Nr 89/08 Wójta Gminy Brudzeń Duży z dnia 31stycznia 2008 roku w sprawie wprowadzenia do użytku służbowego instrukcji dotyczącej ochrony danych osobowych w Urzędzie Gminy Brudzeń Duży.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
inż. Henryk Kisielewski

Załącznik do Zarządzenia nr 159/2008
Wójta Gminy Brudzeń Duży
z dnia 10 grudnia 2008 roku

SPIS TREŚCI

WSTĘP

Administrator Danych dołoży wszelkich starań celem zapewnienia bezpieczeństwa danych i informacji w Urzędzie Gminy w Brudzeniu Dużym. Świadomy wagi zagrożeń, w tym zwłaszcza zagrożeń 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 i inne)
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 i informacje, niezamknięcie na klucz pokoju po jego opuszczeniu, nieoddanie klucza na przechowanie),
   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 Systemów Informatycznych.

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.),
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 Brudzeń Stary,

4) **Administratorze Bezpieczeństwa Informacji** (*ABI*) – należy przez to rozumieć Sekretarza Gminy Brudzeń Duży pisemnie wyznaczonego przez **Wójta Gminy Brudzeń Duży - Administratora Danych** do nadzorowania przestrzegania zasad przetwarzania danych oraz wymagań w zakresie ich ochrony, określonych w Polityce Bezpieczeństwa oraz wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych,
5) **Administratorze Systemów Informatycznych** (*ASI*) – należy przez to rozumieć informatyka Urzędu Gminy pisemnie wskazanego przez **Wójta Gminy Brudzeń Duży - Administratora Danych** do nadzorowania funkcjonowania systemów informatycznych oraz stosowania technicznych i organizacyjnych środków ochrony użytkowanych w tych systemach,
6) **Administratorach Informacji** (*AI*)– należy przez to rozumieć Sekretarza Gminy oraz Skarbnika Gminy decydujących o narzędziach, metodach, miejscu i czasie przetwarzania, przechowywania, tworzenia i niszczenia informacji chronionych w komórkach organizacyjnych,
7) **Użytkownikach Informacji** (*UI*)– należy przez to rozumieć upoważnionych na piśmie pracowników Urzędu Gminy Brudzeń Duży, którym nadano identyfikator i przyznano hasło, mających dostęp do danych. 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 Brudzeń Duży 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, 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,
11) **Systemie tradycyjnym** – należy przez to rozumieć wszelką dokumentację papierową zawierającą informacje o funkcjonowaniu Urzędu Gminy w Brudzeniu Dużym lub jego interesantach - rejestry, ewidencje, księgi, wykazy oraz inne zbiory danych, w tym korespondencję z interesantami Urzędu Gminy w Brudzeniu Dużym,
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 systemów informatycznych Urzędu Gminy Brudzeń Duży 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 osoby, polegająca na podaniu identyfikatora osoby upoważnionej oraz związanego z nim hasła,

18) **Rozliczalności** - należy przez to rozumieć właściwość zapewniającą, że działania mogą być przypisane w sposób jednoznaczny tylko Urzędowi Gminy Brudzeń Duży,
19) **Integralności danych** - należy przez to rozumieć właściwość zapewniającą, że dane osobowe 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 Brudzeń Duży ma na celu zabezpieczenie przetwarzanych danych, 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 Brudzeń Duży w obszarze obsługi interesantów oraz jego funkcjonowania. Niniejsza polityka ustala sposób ochrony danych, zbiór zasad i procedur ich przetwarzania w tych systemach oraz prawa, obowiązki i odpowiedzialność osób upoważnionych do dostępu od 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 22 stycznia 1999 roku o ochronie informacji niejawnych (tj. Dz. U. z 2005 roku, Nr 196, poz. 1631 z póź. zm.) lub informacje chronione ze względu na ważny interes Urzędu Gminy w Brudzeniu Dużym.
W związku z tym, że w systemach przetwarzania znajdują się między innymi dane wrażliwe, a systemy informatyczne posiadają szerokopasmowe połączenie z Internetem, Polityka Bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa.
Osobą odpowiedzialną za bezpieczeństwo informacji chronionych, w tym za ochronę oraz właściwy i niezakłócony przebieg przetwarzania danych w tych systemach jest Administrator Bezpieczeństwa Informacji.

3. Zakres stosowania

Polityka Bezpieczeństwa dotyczy danych przetwarzanych w sposób tradycyjny(papierowy) w rejestrach, ewidencjach, księgach, wykazach i innych zbiorach oraz korespondencji z interesantami Urzędu Gminy Brudzeń Duży (w tym formularzy zgody na przetwarzanie danych osobowych), jak i w systemach informatycznych,
Żasady i procedury określone w Polityce Bezpieczeństwa stosuje się do wszystkich uczestników systemu bezpieczeństwa informacji oraz innych osób mogących mieć dostęp do danych i informacji lub obszarów i pomieszczeń ich przetwarzania.

II. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

W celu zapewnienia bezpieczeństwa oraz ochrony danych przetwarzanych w Urzędzie Gminy Brudzeń Duży ustala się system ochrony danych, w tym danych osobowych, który przedstawiono w **załączniku nr 1** do Polityki Bezpieczeństwa.

1. Administrator Danych realizuje zadania w zakresie:

1) Podejmowania decyzji o celach i środkach przetwarzania danych osobowych i informacji z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji oraz technik zabezpieczenia danych i informacji, w tym danych osobowych,
2) Upoważniania poszczególnych osób do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi ich obowiązków (zadań),
3) Wyznaczenia Administratora Bezpieczeństwa Informacji oraz określanie zakresu jego zadań i obowiązków,
4) Wskazania Administratora Systemów Informatycznych oraz określanie zakresu jego zadań i obowiązków,
5) Podejmowania działań i decyzji w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych i informacji oraz procedur bezpiecznego ich przetwarzania.
6) zgłaszania zbiorów danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

2. **Administrator Bezpieczeństwa Informacji** jest odpowiedzialny za bezpieczeństwo danych, w tym za ochronę oraz właściwy i niezakłócony przebieg przetwarzania tych danych w systemach przetwarzania. Realizuje zadania w zakresie:
   1) przygotowania Polityki Bezpieczeństwa i jej aktualizacji,
   2) przygotowania Instrukcji Zarządzania Systemami Informatycznymi i jej aktualizacji,
   3) wnioskowania o wskazanie Administratora Systemów Informatycznych,
   4) nadzoru nad wdrożeniem i stosowaniem środków fizycznych oraz organizacyjnych i technicznych, w celu zapewnienia bezpieczeństwa danych tj. przed nieautoryzowanym dostępem, kradzieżą, modyfikacją, zatajeniem bądź utratą,
   5) zatwierdzania zmian oraz modyfikacji procedur i regulaminów,
   6) zatwierdzenia wykazu informacji chronionych,
   7) zatwierdzania listy urządzeń i systemów połączonych z siecią Internet,
   8) dokonywania okresowych kontroli przestrzegania przepisów o ochronie danych osobowych,
   9) nadzorowania, pod względem bezpieczeństwa, pracy administratorów informacji oraz Administratora Systemów Informatycznych,
   10) identyfikacji informacji chronionych wynikających z przepisów prawa,
   11) zatwierdzania Imiennych Dokumentów Uprawnień, przygotowywanych przez administratorów informacji, dotyczących przyznania, modyfikacji lub cofnięcia uprawnień do dostępu do informacji,
   12) prowadzenia ewidencji osób upoważnionych do przetwarzania danych,
   13) przygotowywania i prowadzenia szkoleń z zakresu ochrony danych osób dopuszczonych do ich przetwarzania,
   14) nadzorowania przygotowania wniosków zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz prowadzenia innej korespondencji z Generalnym Inspektorem Ochrony Danych Osobowych,
   15) analizowania raportów wszelkich zdarzeń związanych z bezpieczeństwem informacji ochronionych otrzymywanych od Administratora Systemów Informatycznych oraz administratorów informacji,
   16) podejmowania odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych lub procedur bezpieczeństwa przetwarzania,
   17) informowania Administratora Danych o naruszeniach bezpieczeństwa danych oraz procedur bezpiecznego ich przetwarzania,
   18) nadzorowania udostępniania danych odbiorcom danych i innym podmiotom,
   19) przygotowywania, w porozumieniu z Administratorem Systemów Informatycznych, wniosków i propozycji zapotrzebowania na środki finansowe związane z doskonaleniem metod zabezpieczenia technicznego systemów ochrony informacji,
   20) pełnienia funkcji Administratora Informacji w odniesieniu do użytkowników informacji określonych w strukturze ochrony stanowiącej **załącznik nr 1**.
3. **Administrator Systemów Informatycznych** wykonuje zadania w zakresie zarządzania i bieżącego nadzoru nad funkcjonowaniem systemów informatycznych w Urzędzie Gminy, a zwłaszcza:
   1) dbałości o poprawne i efektywne działanie administrowanych systemów,
   2) udostępnianie zasobów informatycznych takich jak foldery, drukarki itp.,
   3) decydowanie o instalacji nowych elementów w systemach,
   4) stosowanie ochrony antywirusowej,
   5) zarządzanie systemami informatycznymi, w których przetwarzane są dane, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji Administratora Systemów Informatycznych,
   6) nadawanie użytkownikom informacji identyfikatorów i haseł dostępu do systemów informatycznych oraz ich zmiana,

7) przydzielanie ściśle określonych praw dostępu w danym systemie oraz określanie uprawnień dla poszczególnych uczestników systemu bezpieczeństwa informacji,
8) modyfikacji uprawnień, usuwanie kont oraz wyrejestrowywanie użytkowników zgodnie z zasadami określonymi w Instrukcji Zarządzania Systemami Informatycznymi,
9) nadzorowanie uwierzytelniania w systemie użytkowników informacji,
10) prowadzenie rejestru osób dopuszczonych do systemów,
11) prowadzenie rejestru zmian haseł użytkowników systemów(programów),
12) prowadzenie rejestru oprogramowania udostępnionego użytkownikom,
13) zmienianie w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie uprawnionemu użytkownikowi informacji,
14) przeciwdziałanie dostępowi osób nieupoważnionych do systemów informatycznych, w których przetwarzane są dane,
15) sprawowanie nadzoru nad wykonywaniem kopii zapasowych, ich przechowywaniem, weryfikowanie ich poprawności oraz okresowe sprawdzanie pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
16) prowadzenie rejestru wykonanych kopii,
17) określanie cyklów oraz nośników archiwizowania danych,
18) sprawowanie nadzoru nad wykonywaniem napraw urządzeń, dysków i innych elektronicznych nośników informacji, ich konserwacją oraz likwidacją,
19) sprawowanie nadzoru nad prawidłowym przeprowadzaniem przeglądów programów i narzędzi programowych systemów,
20) monitorowanie na bieżąco błędów systemów oraz przeglądania rejestrów zdarzeń systemowych,
21) przygotowywanie procedur kryzysowych związanych z incydentami bezpieczeństwa,
22) informowanie Administratora Bezpieczeństwa Informacji w sytuacji stwierdzenia naruszenia zabezpieczeń systemów informatycznych oraz współdziałanie z nim przy usuwaniu skutków naruszenia,
23) prowadzenie szczegółowej dokumentacji naruszeń bezpieczeństwa danych przetwarzanych w systemach informatycznych,
24) wnioskowanie o zatwierdzenie listy urządzeń i systemów połączonych z siecią Internet,
25) wnioskowanie o zatwierdzenie wykazu informacji chronionych,
26) podejmowanie działań służących zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji,
27) przygotowywanie propozycji zapotrzebowania na środki finansowe.

4. **Administrator Informacji** realizuje zadania w zakresie:
   1) decydowania o narzędziach, metodach, miejscu i czasie przetwarzania, przechowywania, tworzenia i niszczenia danych, w tym:
      a) nadzoru nad udostępnianiem danych,
      b) kontrolowania dostępu do danych,
      c) dokonywania kwalifikacji informacji jako chronionych oraz pisemne zobowiązywanie użytkowników informacji do ich kopiowania w sposób określony przez Administratora Systemów Informatycznych,
      d) dokonywania oceny przechowywanych danych pod kątem ich przydatności i ważności dla obsługi interesantów oraz funkcjonowania Urzędu Gminy,
      e) decydowania o usunięciu przechowywanych danych,
      f) decydowania o przetwarzaniu danych w zbiorach doraźnych oraz o ich usunięciu,
   2) przeciwdziałania dostępowi osób nieupoważnionych do systemów przetwarzania, w których przetwarzane są dane,
   3) wnioskowania o nadanie uprawnień do przetwarzania danych osobom, które w związku z wykonywanymi obowiązkami będą miały dostęp do danych i informacji chronionych,

4) przygotowywania Imiennego Dokumentu Uprawnień dotyczącego przyznania, modyfikacji lub odebrania upoważnienia do dostępu do informacji chronionych,
5) przygotowywania dla osób upoważnionych do przetwarzania danych aneksów do indywidualnych zakresów czynności,
6) przygotowywania, w porozumieniu z Administratorem Bezpieczeństwa Informacji, wniosków zgłoszenia zbiorów do rejestracji do Generalnego Inspektora Ochrony Danych Osobowych,
7) ścisłego współdziałania z Administratorem Bezpieczeństwa Informacji dotyczącego przestrzegania zasad ochrony informacji podległych użytkowników informacji,
8) ścisłego współdziałania z Administratorem Systemów Informatycznych dotyczącego funkcjonowania systemów informatycznych,
9) przyjmowania od użytkowników informacji oświadczeń o znajomości przepisów prawa o ochronie danych, zobowiązującego do ich przestrzegania i stosowania,
10) przyjmowania od użytkowników informacji oświadczeń o dotyczących obowiązku ochrony danych osobowych zobowiązującego do zachowania tajemnicy i poufności danych oraz sposobów ich zabezpieczenia,
11) nadzoru nad przestrzeganiem przez użytkowników informacji regulaminów i procedur ochrony informacji,
12) decydowania o przechowywaniu oraz niszczeniu wydruków zawierających dane ważne dla obsługi interesantów oraz funkcjonowania Urzędu Gminy.

5. **Użytkownik Informacji** upoważniony do przetwarzania danych jest zobowiązany do:
1) przetwarzania danych wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych w imiennym upoważnieniu i tylko w celu wykonywania nałożonych obowiązków. Zakres dostępu do danych przypisany jest do identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Odebranie imiennego upoważnienia do przetwarzania danych i informacji powoduje odebranie identyfikatora oraz wygaśnięcie uprawnień i prawa dostępu do systemu,
2) zachowania tajemnicy danych oraz przestrzegania 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) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemami Informatycznymi obowiązującymi w Urzędzie Gminy,
4) znajomości i stosowania określonych procedur i regulaminów dotyczących zgodnego z prawem przetwarzania danych oraz zasad ich ochrony,
5) korzystania 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) zabezpieczania danych przed ich udostępnieniem osobom nieupoważnionym,
7) podpisania aneksu do indywidualnego zakresu czynności,
8) podpisania oświadczenia o znajomości przepisów prawa o ochronie danych, zobowiązującego do ich przestrzegania i stosowania,
9) podpisania oświadczenia dotyczącego obowiązku ochrony danych osobowych zobowiązującego do zachowania tajemnicy i poufności danych oraz sposobów ich zabezpieczenia,
10) uczestniczenia w okresowych szkoleniach dotyczących zasad ochrony danych,
11) uwierzytelnienia się w systemie zgodnie z przyznanym upoważnieniem,
12) bezwzględnego przestrzegania procedur rozpoczęcia, zawieszenia i zakończenia pracy w systemie,

13) kopiowania danych, zgodnie pisemnym zobowiązywaniem, w sposób określony przez Administratora Systemów Informatycznych,
14) przechowywania wymiennych, elektronicznych, nośników informacji w sposób uniemożliwiający nieautoryzowany dostęp do nich,
15) przechowywania dokumentacji papierowej przetwarzanych informacji zgodnie z zasadami określonymi w Polityce Bezpieczeństwa,
16) przechowywania wydruków zawierających dane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych,
17) udostępniania danych zgodnie z decyzją Administratora Danych lub Administratora Informacji,
18) niszczenia danych oraz wydruków zgodnie z decyzją Administratora Informacji,
19) informowania Administratora Systemów Informatycznych o każdej sytuacji odbiegającej od normy w elektronicznych systemach przetwarzania,
20) informowania Administratora Informacji oraz Administratora Bezpieczeństwa Informacji o każdej sytuacji odbiegającej od normy związanej z przetwarzaniem dokumentacji papierowej,
21) możliwie pełnego dokumentowania stwierdzonego zdarzenia mogącego mieć wpływ na bezpieczeństwo danych (np. zapisania treści komunikatów wyświetlanych na monitorze),
22) zgłaszania Administratorowi Systemów Informatycznych potrzeby przeprowadzenia konserwacji oprogramowania,
23) powstrzymywania się przed dokonywaniem jakichkolwiek zmian w konfiguracji sprzętowej urządzeń.

6. **Osoby zobowiązane do zabezpieczenia danych i informacji** przetwarzanych w Urzędzie Gminy (konserwator, sprzątaczki) posiadają imienne upoważnienia Administratora Danych do dostępu do obszarów i pomieszczeń przetwarzania danych i informacji, a do ich obowiązków należy:
   1) nieujawnianie osobom postronnym procedur i sposobów zabezpieczenia i ochrony danych i informacji stosowanych w Urzędzie Gminy w Brudzeniu Dużym,
   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 oraz 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) 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) Obszary ochrony systemów przetwarzania danych i informacji stanowią pokoje określone w **załączniku nr 2** do Polityki Bezpieczeństwa.
2) Kopie zapasowe informacji oraz zbiorów danych przetwarzanych w systemach informatycznych przechowywane są w pomieszczeniu, które stanowi obszar bezpieczny. Dostęp do pomieszczenia posiada Administrator Systemów Informatycznych, Administrator Bezpieczeństwa Informacji oraz Inspektor ds. obronnych, obrony cywilnej

i zarządzania kryzysowego

3) Dokumentacja papierowa przetwarzanych danych przechowywana jest w pokojach stanowiących obszar ochrony systemów przetwarzania.

2. **Zbiory przetwarzanych danych i informacji (informatycznych i papierowych)**

1) W systemach przetwarzania zbierane są dane zawierające informacje o interesantach oraz funkcjonowaniu Urzędu Gminy Brudzeń Duży.

2) Wykaz systemów informatycznych oraz przetwarzanych zbiorów danych stanowi **załącznik nr 3** do Polityki Bezpieczeństwa.

3) Wykaz zbiorów danych przetwarzanych w systemach tradycyjnych (papierowych) stanowi **załącznik nr 4** do Polityki Bezpieczeństwa.

IV. STRUKTURA ZBIORÓW PRZETWARZANYCH W SYSTEMACH

Opis struktury zbiorów przetwarzanych w systemach informatycznych stanowi **załącznik nr 5** do Polityki Bezpieczeństwa.

V. PRZEPŁYW DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI EKSPLOATOWANYMI W URZĘDZIE GMINY BRUDZEŃ DUŻY

1) Poszczególne systemy informatyczne funkcjonujące w Urzędzie Gminy Brudzeń Duży nie są ze sobą powiązane. Dane z poszczególnych systemów nie zasilają się wzajemnie.

2) W przyszłości Administrator Danych dopuszcza przepływ danych pomiędzy systemami. 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 Brudzeń Duży.

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 BRUDZEŃ DUŻY

1. **Bezpieczeństwo osobowe**

1) Administrator Danych prowadzi nabór na stanowiska urzędnicze w drodze konkursu. Kandydaci na pracowników są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także kwalifikacji moralnych. Zwraca uwagę na takie cechy kandydata, jak: uczciwość, odpowiedzialność, przewidywalność zachowań.

2) Ryzyko zagrożenia bezpieczeństwa przetwarzanych danych pojawiające się ze strony osób, które mają do nich dostęp, jest minimalizowane przez zobowiązywanie tych osób do zachowania tajemnicy na podstawie pisemnych oświadczeń.

3) Ryzyko zagrożenia bezpieczeństwa przetwarzanych danych pojawiające się ze strony osób, które mogą uzyskać dostęp do danych (np. osoby sprzątające pomieszczenia), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie pisemnych oświadczeń.

4) Każdy użytkownik informacji przed przystąpieniem do przetwarzania danych i informacji 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) Zarządzeniem Nr 159/2008 Wójta Gminy Brudzeń Duży z dnia 10 grudnia 2008 roku w sprawie Polityki Bezpieczeństwa w Urzędzie Gminy Brudzeń Duży,

d) Zarządzeniem Nr 160/2008 Wójta Gminy Brudzeń Duży z dnia 10 grudnia 2008 roku w sprawie Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Gminy Brudzeń Duży,

e) Podstawowymi zagrożeniami związanymi z przetwarzaniem danych i informacji oraz zastosowanymi środkami technicznymi i organizacyjnymi w celu ich ochrony.

5) Każda osoba dopuszczona do przetwarzania danych i informacji, posiada pisemne upoważnienie Administratora Danych do przetwarzania. W procesie przyznawania upoważnień do przetwarzania danych uczestniczą Administrator Danych, Administrator Bezpieczeństwa Informacji, Administrator Systemów Informatycznych oraz Administratorzy Informacji:

a) Administrator Danych 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.

Uwaga: Szczegółową procedurę nadania uprawnień do przetwarzania danych w systemach informatycznych określono w Instrukcji Zarządzania Systemami Informatycznymi
Uwaga: 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 tej strefy wchodzą:

a) pomieszczenie z serwerem (pokój 7), w którym mogą przebywać wyłącznie Administrator Bezpieczeństwa Informacji, Administrator Systemów Informatycznych, Inspektor ds. obronnych, obrony cywilnej i zarządzania kryzysowego oraz Inspektor ds. obsługi Rady i organów samorządowych. Inne osoby upoważnione do przetwarzania danych i informacji oraz osoby postronne mogą przebywać w pomieszczeniu tylko w ich towarzystwie. Klucz do pomieszczenia jest przechowywany w Sekretariacie Urzędu Gminy,

b) pomieszczenia księgowości z kasą pancerną (pokój 4), w którym mogą przebywać upoważnieni pracownicy księgowości. Inni użytkownicy informacji oraz osoby postronne mogą przebywać w pomieszczeniu tylko w ich towarzystwie. Klucz do pomieszczenia jest przechowywany w Sekretariacie Urzędu Gminy,

c) pomieszczenie Kancelarii Tajnej, w którym może przebywać wyłącznie Pełnomocnik ds. Ochrony Informacji Niejawnych oraz kierownik Kancelarii Tajnej. Osoby postronne w ogóle nie mają dostępu do pomieszczenia.

2) W strefie bezpieczeństwa klasy II dostęp do danych i informacji mają wszystkie osoby upoważnione do przetwarzania, zgodnie z zakresem upoważnienia do ich przetwarzania.

Osoby postronne mogą w niej przebywać wyłącznie w obecności osób upoważnionych do przetwarzania danych i informacji.

Strefa ta obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych i informacji określone w **załączniku nr 2** do Polityki Bezpieczeństwa.

3. Zasady zabezpieczeń stosowane przez Administratora Danych

1) Serwer jest zlokalizowany w pomieszczeniu Nr 7, zamykanym drzwiami zwykłymi. W pomieszczeniu mogą przebywać Administrator Bezpieczeństwa Informacji, Administrator Systemów Informatycznych oraz Inspektor ds. obsługi Rady i organów samorządowych
2) Wszystkie urządzenia systemów informatycznych są zasilane za pośrednictwem zasilaczy awaryjnych (UPS).
3) Okablowanie sieciowe zostało zaprojektowane w ten sposób, że dostęp do linii teletransmisyjnych jest możliwy tylko z pomieszczeń zamykanych na klucz. Ponadto kable sieciowe nie krzyżują się z okablowaniem zasilającym, co zapobiega interferencjom.
4) Bieżąca konserwacja sprzętu informatycznego wykorzystywanego do przetwarzania danych i informacji prowadzona jest wyłącznie przez pracowników Urzędu Gminy.
5) Inne poważne naprawy wykonywane przez osoby z zewnętrz, realizowane w siedzibie Urzędu Gminy, po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary za naruszenie bezpieczeństwa danych.
6) Administrator Systemów Informatycznych dopuszcza konserwację i naprawę sprzętu informatycznego poza siedzibą Urzędu Gminy. W takim przypadku, przed przekazaniem sprzętu, wymontowywane są z niego nośniki informacji zawierające dane i informacje chronione.
7) Zużyty sprzęt informatyczny służący do przetwarzania może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów) właściwym podmiotom, po zawarciu umowy powierzenia przetwarzania danych.
8) 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, należy wymontować nośnik, a następnie zniszczyć.
9) Rejestracji podlegają wszystkie przypadki awarii systemów informatycznych, działania konserwacyjne w systemach oraz naprawy systemów. Są one opisywane w stosownych protokołach, podpisywanych przez osoby uczestniczące w tych działaniach, a także Administratora Bezpieczeństwa Informacji.
10) Administrator Systemów Informatycznych podaje do wiadomości użytkownikom informacji zasady postępowania dotyczące zapewnienia prawidłowej eksploatacji systemów informatycznych, 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 i informacji.
11) Duplikaty kluczy do pomieszczeń stanowiących obszar ochrony systemów przetwarzania przechowywane są w zapieczętowanych kopertach, w Kancelarii Tajnej. Prawo pobrania i otwarcia kopert mają Administrator Danych i Administrator Bezpieczeństwa Informacji. Z pobrania duplikatów sporządza się protokół.

4. Zasady bezpieczeństwa do stosowania przez osoby upoważnione

Każda osoba upoważniona do przetwarzania danych i informacji jest zobowiązana do:

1) usytuowania ekranu komputera w taki sposób, by osoby niepowołane nie mogły widzieć jego zawartości, a zwłaszcza nie ustawiać ekranu naprzeciwko wejścia do pomieszczenia,
2) niepozostawiania bez nadzoru i kontroli dokumentów, nośników danych w miejscach publicznych oraz w samochodach,
3) dbania o prawidłową wentylację komputerów (nie zasłaniania kratek wentylatorów meblami, zasłonami lub stawiania tuż przy ścianie),
4) niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie łatwo powodujących spięcia (grzejniki, czajniki, wentylatory, itp.),
5) należytego pilnowania dokumentów, dyskietek, pamięci przenośnych i komputerów przenośnych,
6) kasowania danych po ich wykorzystaniu, szczególnie na dyskach przenośnych, zgodnie z określoną procedurą,
7) niezapisywania hasła wymaganego do uwierzytelnienia się w systemie w miejscu widocznym i dostępnym (na papierze lub innym nośniku),
8) powstrzymywania się od ingerencji w oprogramowanie i konfigurację powierzonego sprzętu (szczególnie komputerów przenośnych) nawet, gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych,
9) przestrzegania swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń Administratora Bezpieczeństwa Informacji oraz Administratora Systemów Informatycznych,
10) opuszczania stanowiska pracy dopiero po aktywowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób,
11) kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków służbowych przez pracownika. 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 należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane,
12) udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej, zgodnie z określoną procedurą,
13) niewynoszenia poza siedzibę Urzędu Gminy na jakichkolwiek nośnikach całych zbiorów danych i informacji oraz wypisów z nich, nawet w postaci zaszyfrowanej,
14) wykonywania kopii roboczych danych, na których się pracuje, z częstotliwością, która zapobiegnie ich utracie,
15) zakończenia pracy na stacji roboczej, po zapisaniu przetwarzanych danych w odpowiedniej bazie, a następnie prawidłowym wylogowaniu się i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie,
16) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane, bez obecności osoby upoważnionej do przetwarzania,
17) zachowania tajemnicy danych, w tym także wobec najbliższych,
18) niepodawania w rozdzielniku decyzji informacji o adresach stron. Należy stosować rozdzielniki do decyzji, które pozostają w aktach sprawy.
19) niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy,
20) chowania do zamykanych na klucz szaf wszelkich akt zawierających dane przed opuszczeniem miejsca pracy oraz po zakończeniu dnia pracy,
21) umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu, po zakończeniu dnia pracy,

22) zamykania okien w razie opadów lub innych zjawisk atmosferycznych, które mogą zagrozić sprzętowi informatycznemu lub bezpieczeństwu danych,
23) zamykania okien w przypadku opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy,
24) zamknięcia drzwi na klucz po zakończeniu dnia pracy i oddania klucza na przechowanie. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów zawierających dane w zamykanych szafach, należy powiadomić o tym przełożonego, który podejmuje decyzję o postępowaniu związanym z wykonaniem sprzątania pomieszczenia. W takim przypadku także należy zostawić klucz na przechowanie.

5. Postępowanie z nośnikami i ich bezpieczeństwo

1) Dane z nośników przenośnych, niebędących kopiami zapasowymi, po wprowadzeniu do systemów informatycznych Administratora Danych muszą być trwale usuwane z tych nośników przez fizyczne ich zniszczenie lub usunięcie programem trwale usuwającym pliki.
2) Jeśli istnieje uzasadniona konieczność, pojedyncze dane osobowe lub informacje (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na nośnikach przenośnych specjalnie oznaczonych.
3) Nośniki o których mowa w pkt. 2) powinny być oznaczone w sposób następujący:
   a) „Kopia czasowa z programu/zbioru……"
   b) data wprowadzenia danych lub informacji na nośnik,
   c) imię i nazwisko osoby odpowiedzialnej za wprowadzenie danych lub informacji na nośnik,
   d) data przydatności danych lub informacji.
   Nośniki te są przechowywane w szafach zamykanych na klucz, niedostępnych osobom nieupoważnionym. Po ustaniu przydatności tych danych lub informacji muszą być one trwale kasowane lub nośniki zniszczone,
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 i informacje chronione.
   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, ani też wynosić poza siedzibę Urzędu Gminy.

6. Wymiana danych i ich bezpieczeństwo

1) Bezpieczeństwo danych, a w szczególności ich integralność i dostępność, w dużym stopniu zależy od zdyscyplinowanego, codziennego umieszczania/zapisywania danych w odpowiedniej bazie. Pozwoli to, przynajmniej w pewnym stopniu, uniknąć wielokrotnego wprowadzania tych samych danych do systemów informatycznych,
2) Sporządzanie kopii zapasowych następuje w trybie opisanym w **rozdziale VII** Instrukcji Zarządzania Systemami Informatycznymi,
3) Inne wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi producentów sprzętu i używanych programów, wskazówkach Administratora Bezpieczeństwa Informacji, Administratora Systemów Informatycznych oraz Instrukcji Zarządzania Systemami Informatycznymi,
4) Pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko w postaci zaszyfrowanej. Chroni to przesyłane dane przed „przesłuchami" na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w Internecie,
5) Przed atakami z sieci zewnętrznej wszystkie komputery Administratora Danych chronione są środkami dobranymi przez Administratora Systemów Informatycznych w porozumieniu

z Administratorem Bezpieczeństwa Informacji. Użytkownicy informacji zobowiązani są do zwracania uwagi na to, czy urządzenie, na którym pracują, żąda aktualizacji zabezpieczeń. O wszystkich tych przypadkach należy bezzwłocznie powiadomić Administratora Systemów Informatycznych oraz umożliwić mu monitorowanie i aktualizację środków (urządzeń, programów) bezpieczeństwa,

6) Administrator Systemów Informatycznych 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 bazy danych. Administrator Bezpieczeństwa Informacji oraz Administrator Systemów Informatycznych 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 bezpieczne strony https://.

7. Udostępnianie danych osobowych

1) Udostępnianie danych osobowych odbiorcom danych może nastąpić wyłącznie na podstawie złożonego wniosku.
   Wniosek ten powinien mieć formę pisemną i zawierać:
   a) oznaczenie wnioskodawcy,
   b) wskazanie przepisów prawa uprawniających do otrzymania lub wiarygodne uzasadnienie potrzeby posiadania danych,
   c) oznaczenie zbioru w którym żądane dane się znajdują,
   d) określenie rodzaju, zakresu i przeznaczenia potrzebnych danych oraz formy ich przekazania lub udostępnienia,
   e) wskazanie imienia, nazwiska osoby występującej o udostępnienie danych.
2) 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.
3) W przypadku przekazywania informacji na podstawie wniosku ustnego, należy stosownie do okoliczności, zwrócić się z prośbą o ich pokwitowanie albo potwierdzenie odbioru (otrzymania).
4) Osoba udostępniająca dane osobowe jest zobowiązana zażądać pokwitowania pobrania dokumentów przekazanych na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść danych i informacji.
5) Fakt udostępnienia danych osoba udostępniająca jest zobowiązana należy odnotować w systemie informatycznym bądź w prowadzonej ewidencji udostępniania danych.

8. Kontrola dostępu do systemów

1) Pracownikom Urzędu Gminy, konta opatrzone identyfikatorem, umożliwiającym dostęp do danych, przydziela się zgodnie z Imiennym Dokumentem Uprawnień. Administrator Systemów Informatycznych 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 Systemów Informatycznych może przydzielić konto opatrzone identyfikatorem innej osobie, nieposiadającej statusu pracownika Urzędu Gminy.
3) Pierwsze hasło wymagane do uwierzytelnienia w systemie przydzielane jest przez Administratora Systemów Informatycznych, po odebraniu od osoby upoważnionej do przetwarzania danych i informacji oświadczenia zawierającego zobowiązanie do zachowania w tajemnicy pierwszego i następnych haseł oraz potwierdzenia odbioru

pierwszego hasła.

4) Zagwarantowanie poufności i integralności danych i informacji wymaga przestrzegania przez użytkowników informacji swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania wyłącznie własnego identyfikatora i hasła oraz stosowania się do zaleceń Administratora Bezpieczeństwa Informacji i Administratora Systemów Informatycznych.
5) Kontrolę przestrzegania, przez użytkowników informacji, zasad o których mowa w pkt. 4 sprawują Administrator Bezpieczeństwa Informacji oraz Administrator Systemów Informatycznych.

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 zaporę na stacjach roboczych 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) Operacje za pośrednictwem rachunku bankowego może wykonywać wyłącznie pracownik księgowości, upoważniony przez **Administratora Danych,** po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

10. Monitorowanie dostępu do systemów i ich użycia

1) Na stacjach roboczych jest możliwe śledzenie i analiza logów kto, kiedy i jakie programy uruchamia
2) Stacje robocze umożliwiają zapisywanie zdarzeń 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 i innych zasobów systemowych.

11. 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 i informacji, w tym zwłaszcza administratorzy informacji oraz kierownicy referatów, są zobowiązani 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 sporządza się protokół podpisywany przez użytkownika oraz administratora informacji (kierownika referatu), w którym usunięto dane. Protokół zatwierdza Administrator Bezpieczeństwa Informacji.
4) Wzory dokumentów przewidujących powiadomienie, o którym mowa w art. 24 lub 25 ustawy, mogą być stosowane po zaakceptowaniu przez Administratora Bezpieczeństwa Informacji.
5) Administrator Bezpieczeństwa Informacji przygotowuje wykaz zbiorów danych (ewidencyjnych), w którym poszczególnym kategoriom danych przypisane zostały okresy ich przechowywania. Wykaz ten jest sporządzany po przeanalizowaniu przepisów

wyznaczających m.in. obowiązek przechowywania dokumentacji czy też okresy przedawnienia roszczeń udokumentowanych z wykorzystaniem danych.

6) Przed sporządzeniem wykazu, o którym mowa wyżej, należy przygotować wykaz przepisów na mocy, których przetwarzane są dane (sporządzony na podstawie wykazów cząstkowych przygotowanych przez poszczególne komórki organizacyjne).

12. Szkolenia w zakresie ochrony danych

1) Administrator Bezpieczeństwa Informacji przygotowuje i prowadzi szkolenia z zakresu ochrony danych i informacji 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, jeżeli z zakresu ich obowiązków lub działalności wynika konieczność dostępu oraz zabezpieczenia danych,
   d) wszystkie osoby upoważnione do przetwarzania danych, w przypadku każdej zmiany zasad lub procedur ochrony,
2) Tematyka szkoleń obejmuje:
   a) zasady i procedury dotyczące ochrony danych, sporządzania i przechowywania kopii, niszczenia wydruków i zapisów na nośnikach,
   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) zasady i procedury określone w Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemami Informatycznymi.

13. Odpowiedzialność osób upoważnionych do przetwarzania danych

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

14. Zastosowane środki techniczne i organizacyjne

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

1) Środki ochrony fizycznej

a) Dostęp do obszarów przetwarzania informacji mieszczących się w budynku Urzędu Gminy Brudzeń Duży, w godzinach pracy urzędu, nadzorowany jest przez upoważnionych pracowników.
b) Po godzinach pracy dostęp do budynku jest zabezpieczony systemem alarmowym nadzorowanym przez firmę ochrony osób i mienia.
c) Urządzenia służące do przetwarzania informacji znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi.
d) Dokumenty papierowe przetwarzanych informacji chronionych przechowywane są w zamykanych szafach biurowych.
e) Klucze od pokoi są przechowywane w Sekretariacie Urzędu Gminy.
f) Okno w pokoju Kancelarii Tajnej zabezpieczone jest kratami.

g) Zastosowano kasy pancerne do przechowywania kopii zapasowych i wymiennych nośników danych.
h) 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 komputery stacjonarne standardu IBM-PC
b) Zastosowany system operacyjny stacji roboczych – Windows XP, Vista.
c) Serwer bazodanowy jest zlokalizowany w pokoju Nr 7, zabezpieczonym drzwiami zwykłymi. Fizyczny dostęp do serwera posiadają osoby upoważnione: Administrator Bezpieczeństwa Informacji, Administrator Systemów Informatycznych, Inspektor ds. obronnych, obrony cywilnej i zarządzania kryzysowego oraz Inspektor ds. obsługi Rady i organów samorządowych.
d) Zastosowano sieć lokalną przewodową typu Ethernet w topologii gwiazdy.
e) Sieć lokalna jest podłączona do Internetu za pomocą
f) Urządzenia wchodzące w skład systemów informatycznych podłączone są do ogólnego obwodu elektrycznego, a poszczególne stacje robocze wyposażone są w urządzenia podtrzymujące zasilanie - UPS.
g) Zbiory danych prowadzone są w postaci papierowej i elektronicznej.
h) Dane są przetwarzane w sposób zarówno scentralizowany jak i rozproszony.
i) Zastosowano system logowania administratorów i użytkowników informacji do serwera oraz stacji roboczych.
j) Kopie awaryjne wykonywane są na nośnikach CD, DVD lub dyskietkach 3,5".
k) Zastosowano niszczarki dokumentów dla wydruków i materiałów papierowych.

3) **Środki ochrony w ramach oprogramowania urządzeń teletransmisji**
a) Zastosowano programy firewall na stacjach roboczych.
b) Zastosowano działający w „tle" program antywirusowy.
c) Stacje robocze, z których dokonuje się teletransmisji danych, zabezpieczono identyfikatorem, hasłem dostępu oraz przydzieleniem uprawnień w systemie.

4) **Środki ochrony w ramach oprogramowania systemów**
a) Dostęp fizyczny do baz danych zastrzeżony jest wyłącznie dla Administratora Systemów Informatycznych.
b) Konfiguracja systemów umożliwia użytkownikom końcowym dostęp do danych i informacji jedynie za pośrednictwem aplikacji.
c) Zastosowano system uwierzytelnienia użytkowników informacji do stacji roboczych.
d) System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.
e) Zastosowano metody zabezpieczające przed nieuprawnionym dostępem do systemu informatycznego.
f) Zastosowano oprogramowanie umożliwiające wykonanie kopii zapasowych zbiorów danych.
g) Na komputerach użytkowników informacji działa w „tle" program antywirusowy.

5) **Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych**
a) Zastosowano system dostępu za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora i hasła dostępu do danych na poziomie aplikacji.
b) Zastosowano bazy danych –
c) Zastosowano automatyczne rejestrowanie identyfikatora użytkownika.
d) Zastosowano środki umożliwiające określenie praw dostępu do zbiorów.
e) Zdefiniowano użytkowników informacji oraz ich prawa dostępu do danych na poziomie aplikacji.
f) Każdy użytkownik informacji posiada ustalony odrębny identyfikator.

6) **Środki ochrony w ramach systemu użytkowego**

a) Stacje robocze, z których możliwy jest dostęp do danych zabezpieczone są procesem uwierzytelniania, z wykorzystaniem identyfikatora i hasła uruchomieniowego.
b) Zastosowano wygaszacze ekranu w przypadku dłuższej nieaktywności użytkownika.
c) Zastosowano blokady stacji roboczej w przypadku dłuższej nieaktywności użytkownika.

7) **Środki organizacyjne**
a) Wyznaczono Administratora Bezpieczeństwa Informacji – **Barbarę BŁASZKIEWICZ** – Sekretarza Urzędu Gminy Brudzeń Duży (tel. 024-260-40-81 wew. 26). lub 260-40-13
b) Wskazano Administratora Systemów Informatycznych – **Piotra SIECZKOWSKIEGO** – informatyka Urzędu Gminy Brudzeń Duży (tel.024-260-40-13, wew.32).
c) Ustalono Politykę Bezpieczeństwa.
d) Ustalono Instrukcję Zarządzania Systemami Informatycznymi.
e) Prowadzona jest ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych.
f) Określono system nadawania upoważnień oraz dopuszczania osób do przetwarzania danych osobowych.
g) Osoby upoważniane do przetwarzania danych osobowych, przed dopuszczeniem ich do tych danych, są szkolone w zakresie obwiązujących przepisów o ochronie danych osobowych, w tym Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemami Informatycznymi, zasad i procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemach funkcjonujących w Urzędzie Gminy Brudzeń Duży.
h) Do przetwarzania danych dopuszczane są wyłącznie osoby posiadające imienne upoważnienie Administratora Danych, wystawiane na podstawie Imiennego Dokumentu Uprawnień.
i) Ustalono indywidualne zakresy czynności dla osób zatrudnionych przy przetwarzaniu danych osobowych oraz odpowiedzialności za ochronę tych danych.
j) Osoby zatrudnione przy przetwarzaniu informacji, w tym danych osobowych, zobowiązane są do zachowania ich w tajemnicy.
k) Wydruki zawierające dane osobowe nie są wykonywane na drukarce sieciowej.
l) Korespondencja z interesantami jest prowadzona pocztą priorytetową (listy polecone).
m) Zdefiniowano procedury postępowania w sytuacji:
- naruszenia ochrony danych,
- słabości systemu informatycznego,
- niewłaściwego funkcjonowania oprogramowania.
n) W przypadku przetwarzania danych w systemie tradycyjnym (papierowym) stosuje się odpowiednio procedury dotyczące ich przetwarzania w systemach informatycznych.

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 Administrator Bezpieczeństwa Informacji może wcześniej dokonać przeglądu Polityki Bezpieczeństwa.
2) Administrator Bezpieczeństwa Informacji analizuje, czy Polityka Bezpieczeństwa oraz pozostała dokumentacja z zakresu ochrony danych jest adekwatna do:
a) zmian w budowie systemu informatycznego,
b) zmian organizacyjnych w Urzędzie Gminy Brudzeń Duży, w tym również zmian statusu osób upoważnionych do przetwarzania danych,
c) zmian w obowiązującym prawie.
3) Administrator Bezpieczeństwa Informacji po uzgodnieniu z Administratorem Danych może, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z Administratorem Systemów Informatycznych. Zakres, przebieg i wyniki audytu dokumentowane są w protokole podpisywanym przez Administratora Bezpieczeństwa Informacji, Administratora Systemów Informatycznych oraz Administratora Informacji.

4) Administrator Danych, biorąc pod uwagę wnioski Administratora Bezpieczeństwa Informacji, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.

VIII. POSTANOWIENIA KOŃCOWE

1) 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.
2) Każdej osobie upoważnionej do przetwarzania danych i informacji Administrator Bezpieczeństwa Informacji przekazuje wyciąg z Polityki Bezpieczeństwa Informacji, przygotowany z uwzględnieniem jej stanowiska(obowiązków).

Polityka Bezpieczeństwa wchodzi w życie z dniem 10 grudnia 2008 roku

Dokumenty powiązane:
Zarządzenie **Nr160/2008** Wójta Gminy Brudzeń Duży z dnia 10 grudnia 2008 roku w sprawie Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Gminy Brudzeń Duży

Administrator
Bezpieczeństwa Informacji
SEKRETARZ GMINY
B. Błaszkiewicz
Barbara Błaszkiewicz

Załączniki:

Załącznik nr 1
System ochrony informacji Urzędu Gminy w Brudzeniu Dużym
Załącznik nr 2
Obszary ochrony systemów przetwarzania danych i informacji w Urzędzie Gminy Brudzeń Duży
Załącznik nr 3
Wykaz zbiorów danych i informacji przetwarzanych w systemach informatycznych w Urzędzie Gminy Brudzeń Duży
Załącznik nr 4
Wykaz zbiorów danych i informacji przetwarzanych w systemach tradycyjnych (papierowych) w Urzędzie Gminy Brudzeń Duży
Załącznik nr 5
Opis struktury zbiorów przetwarzanych w systemach informatycznych w Urzędzie Gminy Brudzeń Duży