Zarządzenie Nr 36/19

Wójta Gminy Brudzeń Duży

z dnia 30 kwietnia 2019 r.

w sprawie wprowadzenia dokumentacji ochrony danych osobowych

Na podstawie art. 11a ust. 1 pkt 2, art. 31 i art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2019 r. poz. 506) oraz art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie
o ochronie danych) (Dz. Urz. UE L 119 poz. 1), **zarządza się, co następuje**:

§ 1.1. Wprowadza się do realizacji w Urzędzie Gminy w Brudzeniu Dużym dokumentację ochrony danych osobowych.

2. Na dokumentację, o której mowa w ust. 1 składa się:
   1) **Polityka bezpieczeństwa** danych osobowych stanowiąca załącznik nr 1 do niniejszego zarządzenia,
   2) **Instrukcja Zarządzania Systemem Informatycznym** stanowiąca załącznik nr 2 do niniejszego zarządzenia.

§ 2. Zobowiązuje się pracowników Urzędu Gminy w Brudzeniu Dużym przetwarzających dane osobowe do zapoznania się z powyższymi dokumentami i stosowania w pracy zawartych w nich zasad ochrony danych osobowych.

§ 3. Traci moc Zarządzenie Nr 218/18 Wójta Gminy Brudzeń Duży z dnia 23.05.2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik Nr 1 do Zarządzenia Nr 36/19
Wójta Gminy Brudzeń Duży
z dnia 30 kwietnia 2019 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Urząd Gminy w Brudzeniu Dużym
ul. Toruńska 2
09-414 Brudzeń Duży

Data i miejsce sporządzenia dokumentu:	**Brudzeń Duży, dnia 30 kwietnia 2019 r.**
Liczba stron:	**51**
Zatwierdził:	WÓJT Andrzej Dwojnych

SPIS TREŚCI

możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

1.2 Zakres informacji objętych polityką

1. Polityka bezpieczeństwa danych osobowych obejmuje wszystkie dane osobowe oraz inne informacje podlegające ochronie, przetwarzane w Urzędzie Gminy w Brudzeniu Dużym, niezależnie od formy ich przetwarzania. Polityka w zakresie danych osobowych odnosi się:
   1) do danych przetwarzanych w zbiorach tradycyjnych (w wersji papierowej), w szczególności w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
   2) do danych przetwarzanych w systemach informatycznych.
2. Ma ona pomóc w zapewnieniu: poufności, integralności, dostępności oraz rozliczalności przetwarzanych danych osobowych i innych zidentyfikowanych aktywów informacyjnych.
3. Polityka bezpieczeństwa danych osobowych jest jednocześnie dokumentem określającym zadania osób funkcyjnych, pracowników oraz pracowników i współpracowników podmiotów trzecich, które na mocy zawartych umów mają dostęp do informacji chronionych.
4. Niniejsza Polityka bezpieczeństwa danych osobowych zawiera, w formie załączników, wzory dokumentów uszczegóławiających sposób prowadzenia dokumentacji dotyczącej przetwarzania danych osobowych w Urzędzie, np. instrukcje, wytyczne, tabele.
5. Polityka zawiera następujące załączniki:
   1) Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych – Załącznik nr 1
   2) Oświadczenie o zobowiązaniu do zachowania poufności – Załącznik 2a i 2b;
   3) Powołanie Administratora Systemów Informatycznych (ASI) – Załącznik nr 3;
   4) Upoważnienie do przetwarzania danych osobowych – Załącznik nr 4;
   5) Ewidencję wydanych upoważnień do przetwarzania danych osobowych – Załącznik nr 5;
   6) Rejestr zbiorów danych osobowych – Załącznik nr 6;
   7) Wykaz zagrożeń mogących prowadzić do naruszeń – Załącznik nr 7;
   8) Wykaz przykładowych zabezpieczeń – Załącznik nr 8;
   9) Arkusz analizy ryzyka – Załącznik nr 9;
   10) Raport z naruszeń zasad bezpieczeństwa ochrony danych osobowych – Załącznik nr 10;
   11) Rejestr naruszeń i incydentów – Załącznik nr 11;
   12) Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu – Załącznik nr 12;
   13) Upoważnienie do zarządzania kluczami oraz kodem cyfrowym do systemu alarmowego – Załącznik nr 13;
   14) Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe – Załącznik nr 14;
   15) Wykaz zawartych umów o powierzeniu przetwarzania danych osobowych – Załącznik nr 15;
   16) Rejestr czynności przetwarzania – Załącznik nr 16.

w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych;

11) **ograniczenie przetwarzania** – polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
12) **odbiorca –** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią;
13) **podmiot przetwarzający (procesor)** – to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu Administratora;
14) **uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
15) **użytkownik systemu lub osoba upoważniona** – osoba dopuszczona do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, która posiada aktualne, imienne upoważnienie wydane przez Administratora;
16) **szczególne kategorie danych osobowych** – ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życie seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach;
17) **naruszenie ochrony danych osobowych** – jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych;
18) **organ nadzorczy** – rozumie się przez to Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

ROZDZIAŁ 2. Osoby odpowiedzialne za ochronę danych osobowych

2.1 Informacje ogólne

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami rozporządzenia RODO, ustawy, Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy w Brudzeniu Dużym oraz Instrukcji Zarządzania Systemem Informatycznym odpowiadają:

1) Administrator – Wójt Gminy Brudzeń Duży;
2) Zastępca Wójta;
3) Inspektor ochrony danych (IOD);
4) Administrator Systemów Informatycznych (ASI);
5) Kierownicy Referatów Urzędu Gminy w Brudzeniu Dużym;
6) Każda osoba wykonująca pracę bądź świadcząca usługi cywilnoprawne na rzecz Administratora, która uzyskała upoważnienie do przetwarzania danych osobowych.

2.3 Zastępca Wójta

1. Zastępca Wójta Gminy Brudzeń Duży nadzoruje wykonywanie w Urzędzie Gminy zadań wynikających z rozporządzenia RODO, ustawy, Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy w Brudzeniu Dużym oraz Instrukcji Zarządzania Systemem Informatycznym, w szczególności:

1) nadzoruje treść Polityki bezpieczeństwa i Instrukcji;
2) prowadzi nadzór nad fizycznym i organizacyjnym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe;
3) monitoruje działanie i skuteczność zabezpieczeń wdrożonych w celu ochrony danych osobowych;
4) opiniuje w sprawach możliwości oraz prawidłowości zbierania danych osobowych w celu utworzenia zbioru danych osobowych, zbierania nowych kategorii danych do istniejącego już zbioru lub przetwarzania danych w innym celu niż ten, dla którego dane zostały zebrane;
5) opiniuje w sprawach konieczności i stosowanej formie wykonywania obowiązku informacyjnego;
6) wydaje pisemne zalecenia wszelkim osobom przetwarzającym dane osobowe celem przetwarzania ich zgodnie z ustawą, rozporządzeniem, Polityką bezpieczeństwa, Instrukcją;
7) nadzoruje wdrażanie w Urzędzie nowych rozwiązań w zakresie zabezpieczenia danych osobowych;
8) organizuje lub zleca pracownikom Urzędu udział w szkoleniach dotyczących przetwarzania i ochrony danych osobowych;
9) wypełnia obowiązki kontrolne i naprawcze w sytuacjach naruszenia zasad bezpieczeństwa ochrony danych osobowych;
10) nadzoruje pracę Kierowników Referatu pod względem bezpieczeństwa ochrony danych;
11) wykonuje inne czynności przewidziane w niniejszej Polityce bezpieczeństwa.

2. Zastępca Wójta jest zobowiązany do współpracy z Administratorem, IOD, ASI, Kierownikami Referatów w zakresie nadawania, przygotowywania, rejestrowania, zbierania, ewidencjonowania i przechowywania:

1) imiennych upoważnień osób do przetwarzania danych osobowych;
2) ewidencji wydanych upoważnień do przetwarzania danych osobowych w Urzędzie;
3) oświadczeń o zobowiązaniu do zachowaniu poufności;
4) umów powierzenia przetwarzania danych osobowych, w których Gmina jest stroną;
5) wniosków o udostępnienie danych ze zbioru danych osobowych;
6) rejestru zbiorów danych osobowych;
7) dokumentacji dotyczącej analizy ryzyka;
8) raportów naruszeń zasad bezpieczeństwa ochrony danych osobowych;
9) rejestru naruszeń i incydentów;
10) innych pism, dokumentów wymaganych Polityką, Instrukcją, ustawą, rozporządzeniem.

3. Szczegółowy zakres obowiązków Zastępcy Wójta w zakresie ochrony danych osobowych w Urzędzie Gminy w Brudzeniu Dużym określa Regulamin Organizacyjny.

w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z poziomu administratora.

4. Do uprawnień i obowiązków Administratora Systemów Informatycznych należy m. in.:
   1) nadawanie uprawnień do przetwarzania danych osobowych w systemach informatycznych – zakładanie, blokowanie, zawieszanie i uaktywnianie kont;
   2) prowadzenie rejestru nadanych uprawnień do przetwarzania danych w systemach informatycznych;
   3) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów;
   4) nadzorowanie zabezpieczeń systemów informatycznych w zakresie: przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz działań inicjowanych z sieci i z systemu informatycznego;
   5) nadzór nad procedurami przekazywania podmiotowi nieuprawnionemu urządzeń systemów informatycznych oraz elektronicznych nośników informacji zawierających dane osobowe;
   6) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;
   7) identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych;
   8) wyjaśnianie i dokumentowanie przypadków naruszania zasad bezpieczeństwa systemów informatycznych;
   9) wykonywanie kopii zapasowych zbiorów danych zgodnie z zasadami określonymi w Instrukcji oraz okresowo sprawdzanie ich pod kątem dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
   10) nadzór nad niszczonymi i przechowywanymi kopiami zapasowymi zbiorów danych osobowych oraz programów zastosowanych do ich przetwarzania;
   11) osobiste wykonywanie lub nadzorowanie nad wykonywaniem: napraw, konserwacji oraz likwidacji urządzeń komputerowych, które mogą zawierać dane osobowe;
   12) dokonywanie oceny zgodności aplikacji z przepisami bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych;
   13) inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych;
   14) podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych, o których mowa w Instrukcji Zarządzania Systemem Informatycznym;
   15) informowanie Zastępcę Wójta i/lub IOD/Administratora o konieczności wprowadzenia zmian w niniejszej Polityce bezpieczeństwa oraz Instrukcji (np. z powodu zmian procedur tworzenia kopii zapasowych lub zmiany zabezpieczeń systemów informatycznych).

Administrator Systemów Informatycznych ma obowiązek prowadzenia analizy i przedstawiania wniosków dotyczących zmiany czynności organizacyjnych Administratorowi, Zastępcy Wójta i/lub Inspektorowi ochrony danych i wdrażania w systemach informatycznych zabezpieczeń

5) zabezpieczania zbiorów danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w Polityce bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym, niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie;
6) nieudzielania informacji o danych osobowych innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w takich przepisach zostały spełnione;
7) niezwłocznego zawiadamiania Administratora/Inspektora ochrony danych o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających te dane osobowe.

5. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Kodeksu pracy, bądź rozwiązania stosunku cywilnoprawnego łączącego strony.

ROZDZIAŁ 3. Upoważnienia do przetwarzania danych osobowych

1. Upoważnienie do przetwarzania danych osobowych jest dokumentem niezbędnym do tego, aby pracownik Urzędu Gminy w Brudzeniu Dużym mógł przetwarzać w systemie informatycznym lub w wersji papierowej dane osobowe. Upoważnienie nadawane jest indywidualnie, z wyraźnym wskazaniem, jakie zbiory danych obejmuje swoim zakresem. Upoważnienie do przetwarzania danych osobowych nadawane jest przez Administratora.

2. Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu szkolenia z zakresu zasad ochrony danych osobowych, o którym mowa w **Rozdziale 11.** niniejszej Polityki bezpieczeństwa. Osoba, która odbyła szkolenie ma obowiązek złożyć zobowiązanie do zachowania danych w tajemnicy, którego wzór stanowi odpowiednio **Załącznik nr 2a i 2b** do niniejszej Polityki bezpieczeństwa.

3. Po złożeniu zobowiązania pracownikowi/stażyście/praktykantowi, jeżeli jest to konieczne, nadawane jest upoważnienie do przetwarzania danych osobowych. Wzór Upoważnienia do przetwarzania danych osobowych stanowi **Załącznik nr 4** do niniejszej Polityki bezpieczeństwa.

4. Upoważnienie nadawane jest na wniosek bezpośredniego przełożonego danego pracownika/stażysty/praktykanta. We wniosku należy określić indywidualne obowiązki i odpowiedzialności pracownika związane z przetwarzaniem danych osobowych, oraz wskazać do jakich zbiorów danych osobowych pracownik będzie miał dostęp. Wniosek może mieć postać dokumentu papierowego lub może zostać złożony w formie e-maila.

5. Wniosek, o którym mowa w ust. 4 należy przedłożyć do Zastępcy Wójta w celu przygotowania Upoważnienia do przetwarzania danych osobowych. Przygotowane Upoważnienie przedkładane jest Administratorowi w celu zatwierdzenia zakresu upoważnienia i podpisania.

6. Zastępca Wójta informuje ASI o treści podpisanego upoważnienia, o którym mowa w ust. 4 w celu przyznania dostępów do ściśle określonych systemów informatycznych.

4.1 Analiza ryzyka

W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć. Dane osobowe przetwarzane przez Urząd Gminy w Brudzeniu Dużym zawarte są w postaci zbiorów danych osobowych i zostały wykazane w **Załączniku nr 6** do niniejszej Polityki bezpieczeństwa.

4.2 Określenia stosowane w procedurze

1) **Aktywa (zasoby)** – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych. Aktywem jest każdy element, który ma wartość dla organizacji. Mogą to być m.in. pracownicy, outsourcing, sprzęt IT, oprogramowanie (programy i system operacyjny), dane osobowe, infrastruktura, informacje;
2) **Naruszenie (Incydent) ochrony danych osobowych** – to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
3) **Zagrożenie** – potencjalne naruszenie (potencjalny incydent), np. zagrożenie naturalne, losowe, zamierzone, administracyjne;
4) **Prawdopodobieństwo** – prawdopodobieństwo wystąpienia zagrożenia (incydentu) w danym zbiorze danych osobowych/w procesie przetwarzania;
5) **Skutek** – rezultat niepożądanego incydentu (straty jakie poniesie jednostka w wypadku urzeczywistnienia się zagrożenia);
6) **Ryzyko** – prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów (aktywów);
7) **Strata** – np. strata wizerunku jednostki lub zaufania, strata aktywów – w tym również niematerialnych.

4.3 Wyznaczenie zagrożeń

1. Administrator określa listę zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze danych osobowych/w procesie przetwarzania.
2. Zagrożenia są identyfikowane w odniesieniu do wcześniej zidentyfikowanych aktywów (zasobów).
3. Wykaz zagrożeń, które mogą wystąpić w Urzędzie Gminy w Brudzeniu Dużym stanowi **Załącznik nr** 7 do niniejszej Polityki bezpieczeństwa. Nie stanowi on zamkniętego katalogu zagrożeń, które mogą wystąpić w jednostce.

4.4 Wyliczenie ryzyka dla zagrożeń

1. Każde zidentyfikowane zagrożenie podlega analizie mającej na celu oszacowanie prawdopodobieństwa wystąpienia oraz skutku, jaki będzie miało ewentualne wystąpienie tego zagrożenia (ocena punktowa w skali od „1" do „3"):
   1) Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze danych osobowych/w procesie przetwarzania. Sposób określenia prawdopodobieństwa wystąpienia ryzyka obrazuje poniższa tabela:

działania w celu jego obniżenia, wymaga okresowego monitorowania;

3) **6-9 – ryzyko wysokie –** jest ryzykiem nieakceptowanym i wymaga podjęcia zdecydowanych działań w celu zmniejszenia ryzyka do akceptowalnego poziomu, poprzez zmniejszenie jego wpływu lub prawdopodobieństwa wystąpienia.

4.5 Reakcja na ryzyko

1. Administrator przyjmuje następujące sposoby postępowania z ryzykiem:
   1) **akceptacja ryzyka** – zabezpieczenia są wystarczające, nie ma potrzeby wprowadzania zmian w działaniu organizacji (zabezpieczeń);
   2) **transfer ryzyka (przeniesienie)** – przerzucenie ryzyka na podmiot zewnętrzny;
   3) **unikanie** – unikanie działań powodujących występowanie ryzyka;
   4) **redukcja** – działania pozwalające na obniżenie poziomu ryzyka do akceptowalnego.
2. Wykaz przykładowych zabezpieczeń stanowi **Załącznik nr 8** do niniejszej Polityki bezpieczeństwa.
3. Arkusz analizy ryzyka stanowi **Załącznik nr 9** do niniejszej Polityki bezpieczeństwa.

4.6 Ponowna analiza ryzyka

Administrator przeprowadza Analizę ryzyka cyklicznie, tj. raz na rok lub w przypadku wystąpienia znaczących zmian w przetwarzaniu danych (np. przetwarzanie nowych zbiorów danych osobowych, wystąpienie nowych procesów przetwarzania, zmian w przepisach prawnych, zmian w infrastrukturze jednostki).

4.7 Plan postępowania z ryzykiem

1. Tam, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji oraz osoby odpowiedzialne.
2. Administrator wyznacza Administratora Systemów Informatycznych do monitorowania wdrożonych zabezpieczeń technicznych. Za monitorowanie zabezpieczeń organizacyjnych odpowiada Zastępca Wójta.

ROZDZIAŁ 5. Postępowanie z incydentami

Zgodnie z art. 4 pkt 12 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) „naruszenie ochrony danych osobowych" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

b) zdarzenia losowe wewnętrzne (możliwość awarii sprzętu IT (awarie serwera, komputerów, twardych dysków, brak lub awaria ups) lub oprogramowania ze względu na brak odpowiedniego serwisowania, pomyłki informatyków, użytkowników, utrata/zagubienie/przypadkowe zniszczenie danych,
c) umyślne działanie (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania poprzez samowolne instalowanie niedozwolonego oprogramowania na służbowym sprzęcie).

5. Procedurę stosuje się odpowiednio w przypadku stwierdzenia, że stan dokumentacji lub stan pomieszczeń bądź szaf biurowych, w których przechowywana jest dokumentacja wzbudzają podejrzenie, że dostęp do nich mogły mieć osoby nieupoważnione.

5.2 Postępowanie w przypadku naruszenia danych osobowych

1. Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek zgłosić przypadek naruszenia danych bezpośredniemu przełożonemu oraz podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony, zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia. Bezpośredni przełożony niezwłocznie informuje o zaistniałej sytuacji Zastępcę Wójta, Inspektora ochrony danych (IOD) i Administratora Systemów Informatycznych (ASI). Do czasu przybycia IOD i (ASI), bądź innej osoby upoważnionej przez Administratora, pracownik:
a) zabezpiecza dostęp do miejsca lub urządzenia,
b) wstrzymuje pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, które w związku z naruszeniem ochrony zostały wstrzymane,
c) podejmuje, stosownie do zaistniałej sytuacji inne, niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
d) jest zobowiązany zaniechać wszelkich innych działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia ,
e) nie opuszcza bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora ochrony danych (IOD) i/lub Administratora Systemów Informatycznych (ASI), bądź innej osoby upoważnionej przez Administratora.

2. Dokonywanie zmian w miejscu naruszenia ochrony danych, o których mowa w pkt 1, bez uzyskania zgody jest dopuszczalne, jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.

3. Zgodę na ponowne uruchomienie komputerów i innych urządzeń oraz kontynuowanie pracy przy pomocy sprzętu IT wyraża Administrator Systemów Informatycznych.

4. Administrator Systemu Informatycznego jest zobowiązany do informowania Inspektora ochrony danych i Zastępcy Wójta o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

5. Bezpośredni przełożony pracownika, Zastępca Wójta, IDO i ASI który wykrył lub został poinformowany o nieprawidłowościach przy przetwarzaniu danych osobowych powinien niezwłocznie zidentyfikować problem i przedsięwziąć wszelkie niezbędne kroki, aby uniknąć w przyszłości podobnych zdarzeń.

5.4 Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1. W przypadku wykrycia naruszenia ochrony danych osobowych skutkującego wystąpieniem ryzyka naruszenia praw i/lub wolności osób fizycznych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Wzór Zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu stanowi **Załącznik nr 12** do niniejszej Polityki bezpieczeństwa.

2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

- **a)** opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
- **b)** zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- **c)** opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
- **d)** opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

3. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

5.5 Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2. Zawiadomienie, o którym mowa w ust. 1, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w **dziale 5. 4** ust. 2 lit. b), c) i d).

3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:

- **a)** Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
- **b)** Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
- **c)** wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Witryna internetowa powinna używać prawidłowego certyfikatu bezpieczeństwa.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.
8. Zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych i innych urządzeń dostępowych. Zabrania się łączenia, przy pomocy takich urządze,ń komputerów z Internetem.

6.2. Zasady korzystania z poczty elektronicznej

1. Pracownik może korzystać ze służbowej poczty e-mail tylko w celach związanych z wykonywaniem obowiązków służbowych. Zabrania się wykorzystywać służbowego konta e-mail do celów prywatnych.
2. W celu zalogowania się do służbowej poczty e-mail można wykorzystywać przeglądarkę internetową lub klienta poczty elektronicznej (np. program Microsoft Outlook). Logowanie się do służbowego konta e-mail (przez przeglądarkę internetową lub przez klienta poczty e-mail) musi odbywać się przy użyciu zaszyfrowanego połączenia.
3. Należy unikać przekazywania danych osobowych poprzez pocztę elektroniczną.
4. W przypadku przekazania dokumentu zawierającego dane osobowe pocztą elektroniczną należy dokument ten zabezpieczyć silnym hasłem (zawierającym min. 8 znaków, duże i małe litery oraz cyfry lub znaki specjalne), np. wykorzystując program do archiwizowania dokumentów umożliwiający zabezpieczenie utworzonego archiwum hasłem. Zabezpieczony dokument należy dodać jako załącznik do wiadomości e-mail. Hasło do otworzenia dokumentu należy przekazać inną drogą niż poprzez wiadomość e-mail (np. telefonicznie). Nie wolno przekazywać danych osobowych bezpośrednio w treści wiadomości e-mail, zabrania się umieszczać dokumentów zawierających dane osobowe „w chmurze" i udostępniać tych dokumentów w postaci przesłanego linku do pobrania pliku (lub w jakikolwiek inny sposób) za pośrednictwem poczty elektronicznej.
5. Zaleca się, aby pracownik podczas przesyłania danych osobowych e-mail'em zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. Pracownicy są zobowiązani zwracać szczególną uwagę na poprawność adresu odbiorcy wysyłanej wiadomości.
7. Podczas wysyłania e-mail'i do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie e-maili do wielu adresatów z użyciem opcji „Do wiadomości".
8. Przypadki podejrzanych e-maili należy bezzwłocznie zgłaszać Administratorowi Systemów Informatycznych.
9. Pracownicy zobowiązani są okresowo kasować niepotrzebne e-maile.
10. Pracownicy nie mają prawa korzystać z e-maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
11. Zabrania się udostępniać innym pracownikom dostęp do swojej poczty elektronicznej bez zgody przełożonego.

odpowiedzialną za zorganizowanie pracy pracowników obsługi (sprzątaczek) poza godzinami pracy Urzędu jest Zastępca Wójta.

12. Klucze zapasowe do wszystkich pomieszczeń Urzędu są zabezpieczone i przechowywane w zamkniętej szafce zlokalizowanej w sekretariacie Urzędu. Wydawanie kluczy zapasowych pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz w przypadkach awaryjnych. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do sekretariatu.

13. Raz na kwartał Zastępca Wójta będzie zlecał przeprowadzenie kontroli kompletności kluczy do wszystkich pomieszczeń Urzędu.

14. Otwarcie Urzędu w soboty, niedziele oraz święta możliwe jest wyłącznie w uzasadnionych przypadkach za wiedzą i zgodą Administratora – Wójta Gminy lub Zastępcy Wójta oraz w związku z przeprowadzeniem ceremonii zawarcia małżeństwa.

15. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 Kodeksu pracy oraz z art. 363 §1. Kodeksu cywilnego.

ROZDZIAŁ 7. Obszar w którym przetwarzane są dane osobowe

1. Obszar, w których przetwarzane są dane osobowe obejmuje zarówno miejsca, w których wykonuje się operacje na danych osobowych (np. wpisuje, modyfikuje, kopiuje), jak również miejsca, gdzie przechowuje się wszelkie nośniki zawierające dane osobowe. Wskazując na obszar przetwarzania danych należy uwzględnić także obszar, w którym przetwarzane są dane powierzone przez Administratora odrębnym podmiotom.

2. Budynki i pomieszczenia lub ich części, w których przetwarzane są dane osobowe, powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym, na czas nieobecności osób upoważnionych.

3. Budynki, pomieszczenia lub ich części, o których mowa w ust. 2 posiadają następujące zabezpieczenia:

1) drzwi do pomieszczeń, w których przetwarzane są dane osobowe są zamykane na klucz – w Urzędzie wdrożono Politykę kluczy,
2) dokumenty z danymi osobowymi zamykane są na klucz w szafach,
3) budynek objęty jest monitoringiem: kamery znajdują się na zewnątrz budynku, jak również na korytarzach;
4) budynek objęty jest systemem sygnalizacji alarmu i włamania, do którego szyfr posiadają: Wójt Gminy, Zastępca Wójta, wskazani pracownicy obsługi – Urząd posiada podpisaną umowę z firmą ochroniarską;
5) system sygnalizacji o pożarze jest podłączony do jednostek Policji i Straży Pożarnej.

4. Osoby upoważnione do przetwarzania danych osobowych mogą przetwarzać dane tylko w wyznaczonych do tego miejscach.

5. Wzór Wykazu budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe stanowi **Załącznik nr 14** do niniejszej Polityki bezpieczeństwa.

6. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe powinien być każdorazowo aktualizowany po wprowadzaniu istotnych zmian w strukturze bazy danych, którą opisuje.

bezpieczeństwo przetwarzania w Urzędzie Gminy w Brudzeniu Dużym. W tym celu Administrator przeprowadza audyt wewnętrzny. Celem audytu wewnętrznego jest ocena, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO. Audyt prowadzony jest w sposób obiektywny i bezstronny.

3. Administrator przy współpracy z Inspektorem ochrony danych (IOD) opracowuje plan i program audytów biorąc pod uwagę ważność procesów przetwarzania oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów, jeżeli były prowadzone. Określa on kryteria audytu, jego cel, zakres i ewentualnie metody.

4. Audyt w jednostce przeprowadza się raz na rok. W wyjątkowych sytuacjach Administrator może zażądać przeprowadzenie audytu wcześniej.

5. Audyt przeprowadza Inspektor ochrony danych. Audyt może przeprowadzić także inna osoba wyznaczona przez Administratora.

6. Audytor jest zobowiązany do przygotowania się do przeprowadzenia audytu, zapoznając się z opisem audytowanego obszaru, stosowanych procedur i wyników poprzednich audytów, jeżeli były prowadzone.

7. Audytor realizuje działania audytowe mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań RODO.

8. W przypadku stwierdzenia uchybień mających wpływ na skuteczność działania systemu ochrony danych zgodnego z RODO, audytor identyfikuje tzw. uchybienia lub spostrzeżenia.

9. Po zakończeniu audytu audytor przygotowuje sprawozdanie z przeprowadzonego audytu oraz oceny systemu ochrony i przetwarzania danych osobowych. Sprawozdanie jest przedstawiane Administratorowi, a następnie – po pisemnym przyjęciu do wiadomości przez Administratora – zostaje przedstawione wszystkim pracownikom. Istotnym elementem sprawozdania jest wykaz czynności, które zostaną podjęte przez Administratora w celu wyeliminowania wykrytych nieprawidłowości oraz wdrożenia nowych procedur zgodnych z RODO. Mogą to być np. szkolenia, zakup sprzętu, mebli, niszczarek, ale także przemeblowanie czy przeniesienie dokumentów do innych pomieszczeń.

10. Administrator przy współpracy z Inspektorem ochrony danych dokonuje przeglądu i analizy wyniku audytu oraz decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia poważnych uchybień.

11. Audytorzy nie audytują własnej pracy.

ROZDZIAŁ 11. Szkolenia

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi musi być poddana przeszkoleniu i zapoznana z przepisami rozporządzenia RODO, ustawą o ochronie danych osobowych oraz dokumentacją ochrony danych osobowych wdrożoną przez Administratora w Urzędzie, tj. Polityką bezpieczeństwa danych osobowych oraz Instrukcją Zarządzania Systemem Informatycznym.
2. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania. W tym celu uczestnicy szkolenia podpisują odpowiednie Oświadczenie o zobowiązaniu do zachowania poufności, którego wzór stanowi **Załącznik nr 2a i 2b** do niniejszej Polityki bezpieczeństwa.

ROZDZIAŁ 12. Załączniki

Załącznik nr 1 do Polityki bezpieczeństwa danych osobowych
Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. W Urzędzie Gminy w Brudzeniu Dużym określono środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
2. W Urzędzie zastosowano nw. zabezpieczenia:

I. Środki organizacyjne:

1) Opracowano i wdrożono dokumentację ochrony danych osobowych – Politykę bezpieczeństwa danych osobowych, Instrukcję Zarządzania Systemem Informatycznym.
2) Powołano Inspektora ochrony danych (IOD).
3) Powołano Administratora Systemów Informatycznych (ASI).
4) Do przetwarzania danych osobowych dopuszczono tylko osoby posiadające ważne upoważnienia nadane przez Administratora.
5) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
6) Osoby zatrudnione przy przetwarzaniu danych zaznajomiono z przepisami dotyczącymi ochrony danych osobowych.
7) Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
8) Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązano do zachowania ich w tajemnicy.
9) Monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
10) Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
11) Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
12) Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
13) Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe.
14) W jednostce prowadzi się politykę czystego biurka i ekranu.

II. Środki ochrony fizycznej:

1) Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).
2) Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem kontroli dostępu.
3) Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych usytuowanych na korytarzach Urzędu.

7) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Oświadczenie o zobowiązaniu do zachowania poufności

Ja niżej podpisany/na ..... zatrudniony/(na) na stanowisku ..... w .....
oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz dokumentacją ochrony danych osobowych obowiązującą w Urzędzie Gminy w Brudzeniu Dużym i zobowiązuję się do:

- zachowania w tajemnicy danych osobowych w sytuacji dostępu do nich podczas pełnienia obowiązków służbowych w Urzędzie Gminy w Brudzeniu Dużym wynikających z umowy o pracę/umowy praktyki/umowy stażu/umowy cywilnoprawnej*),
- zabezpieczenia tych danych przed dostępem osób nieupoważnionych, a następnie przekazania ich do dyspozycji osób upoważnionych,
- zgłaszania sytuacji (incydentów) naruszenia ochrony danych osobowych Inspektorowi ochrony danych lub bezpośredniemu przełożonemu.

Jednocześnie oświadczam, że uzyskane, w trakcie wykonywania pracy, informacje zachowam w poufności zarówno w trakcie wykonywania umowy, jak i po jej rozwiązaniu/wygaśnięciu.

miejscowość i data	podpis osoby składającej oświadczenie

Rozdzielnik 3 egz. w oryginale:
1 x oryginał dokumentacja ochrony danych
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba składająca oświadczenie

*) niepotrzebne skreślić

Upoważnienie do przetwarzania danych osobowych Nr .../...

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) jako Administrator w Urzędzie Gminy w Brudzeniu Dużym, ul. Toruńska 2, 09–414 Brudzeń Duży, **upoważniam:**

Panią/Pana*).....

zatrudnioną/nego*) na stanowisku pracy .....w Referacie .....

Urzędu Gminy w Brudzeniu Dużym do przetwarzania danych osobowych w zbiorach:

.....

.....

(nazwy zbiorów danych objętych zakresem upoważnienia)

W zakresie: wglądu, wprowadzania, modyfikacji, usuwania, archiwizacji, udostępniania innym podmiotom, koniecznym do wykonywania obowiązków pracowniczych.*)

Upoważnienie dotyczy przetwarzania danych osobowych w systemach informatycznych: .....

.....

(nawy systemów lub programów)

jak również ww. zbiorach, które są prowadzone wyłącznie w formie tradycyjnej (papierowej).

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. Dz.U.UE.L.2016.119.1), powszechnie obowiązującym prawem oraz obowiązującymi w Urzędzie Gminy w Brudzeniu Dużym wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków stanowi naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu pracy lub odpowiedzialności cywilnej.

Upoważnienie jest ważne do czasu zakończenia stosunku pracy, stosunku cywilnoprawnego lub odwołania.

Ewidencja wydanych upoważnień do przetwarzania danych osobowych

L.p.	Imię i nazwisko osoby upoważnionej	Zajmowane stanowisko służbowe osoby upoważnionej	Numer upoważnienia	Data nadania upoważnienia	Data odwołania/ ustania upoważnienia	Identyfikator w systemie informatycznym	Nazwy zbiorów objętych zakresem upoważnienia
	1	2	3	4	5	6	7
1.							
2.							
3.							
4.							
5.							
6.							
7.							
...							

Wykaz zagrożeń mogących prowadzić do naruszeń

Najczęściej występujące zagrożenia prowadzące do naruszeń to :

1) Organizacyjne:

- brak nadanych upoważnień osobom przetwarzającym dane osobowe,
- brak wdrożonych polityk i procedur dotyczących ochrony danych osobowych,
- brak powołania inspektora ochrony danych osobowych w sytuacji, gdy wyznaczenie jest obligatoryjne,
- nieuprawniony dostęp do pomieszczenia, w którym są przetwarzane dane osobowe.

2) Techniczne:

- atak hakerski,
- działanie złośliwego oprogramowania (wirusy),
- awaria nośników danych,
- awaria sprzętu sieciowego,
- awaria serwera,
- awaria zasilania – brak ups,
- celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych,
- przesłanie danych drogą mailową do złego odbiorcy.

3) Fizyczne:

- pożar, zalanie
- kradzież sprzętu z danymi,
- kradzież danych w wersji papierowej,
- zniszczenie danych osobowych bez użycia niszczarki,
- atak terrorystyczny,
- zwarcie instalacji elektrycznej,
- nieodpowiednie przechowywanie danych,
- utrata przetwarzanych danych,
- niewystarczający poziom zabezpieczenia pomieszczeń.

4) Personalne:

- nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik,
- wejście w posiadanie danych osobowych przez osobę nieuprawnioną,
- udostępnianie danych osobowych osobom nieupoważnionym,
- udostępnianie haseł innym pracownikom,
- nie zachowanie tajemnicy służbowej dotyczącej danych osobowych przez pracowników podczas pracy, jak i po jej zakończeniu,
- otwieranie podejrzanych maili, mogących zawierać wirusy komputerowe,
- nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym.

9	włamanie do sieci WIFI	uzyskanie dostępu do sieci wewnętrznej poprzez włamanie się do niechronionej sieci WIFI
10	brak aktualnej dokumentacji	brak instrukcji obsługi, dokumentacji technicznej sprzętu, instrukcji instalacyjnych i konfiguracyjnych
11	nieprzestrzeganie procedur wprowadzonych w jednostce	świadome niestosowanie się do procedur zawartych w dokumentacji ochrony danych jednostki, przekazywanie haseł do aplikacji z danymi innym osobom
12	nieuprawniony dostęp lub włamanie do pomieszczeń	dostęp do budynku, pomieszczeń biurowych, archiwum, serwerowni, miejsc gdzie przechowywane są kopie zapasowe
		dostęp do wersji papierowych dokumentów zawierających dane, do aplikacji, nośników typu pendrive
		kradzież dokumentów, komputerów, dysków twardych, pendrive
13	kradzież bądź zgubienie nośników danych	kradzież laptopów, pendrive, dysków wymiennych zawierających dane osobowe
14	nieprawidłowe lub brak umowy gwarancyjnej, wsparcia serwisowego	nieprzedłużenie umowy, brak zapisów dotyczących okresu gwarancji, brak zapisów dotyczących reakcji firmy na zgłoszenie
15	eskalacja uprawnień	nadawanie szerszych uprawnień użytkownikom niż wynika to z zakresu czynności, przejęcie uprawnień administratora
16	awarie/uszkodzenia infrastruktury IT	awarie: dysków, stacji roboczych, urządzeń sieciowych, serwera
17	awarie oprogramowania	niedziałający program do spraw kadrowo-płacowych, awaria poczty, strony www, baz danych
18	pożar	pożar całego obiektu, pożar w pomieszczeniu serwerowni/serwera
19	powódź	zalanie pomieszczenia serwerowni, zalanie pomieszczenia archiwum
20	przegrzanie	wysoka temperatura w serwerowni - awaria klimatyzacji i przegrzanie serwera powodujące poważną awarię
21	awaria napięcia	skoki napięcia, przerwy w dostawie zasilania

Arkusz analizy ryzyka

L.p.	Aktywa *(środki materialne i niematerialne)*	Zidentyfikowane zagrożenia	Opis zagrożenia	Prawdopodobieństwo incydentu	Skutki wystąpienia incydentu	Ryzyko wystąpienia incydentu	Zabezpieczenia	
				P *(skala od 1 do 5)*	S *(skala od 1 do 3)*	P x S	*(wdrożone zabezpieczenia w jednostce)*	*(planowane do wdrożenia zabezpieczenia w jednostce)*
1.								
2.								
3.								
4.								
5.								
6.								
7.								
...								

.....

.....

7. Skutki zdarzenia:

.....

.....

.....

.....

8. Postępowanie wyjaśniające:

.....

.....

.....

.....

.....

.....

.....
(data i podpis osoby zgłaszającej)

.....
(data i podpis Inspektora ochrony danych)

.....
(data i podpis Administratora Systemów Informatycznych)

.....
(data i podpis Administratora)

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

1. Data: ..... Godzina: ..... (naruszenia)

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem:

.....

.....
(imię, nazwisko, stanowisko służbowe)

3. Lokalizacja zdarzenia:

.....

.....

.....
(nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.)

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu *(opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie):*

.....

.....

.....

5. Podjęte działania:

.....

.....

.....

6. Wstępna ocena przyczyn wystąpienia naruszenia *(opisywać możliwe konsekwencje naruszenia ochrony danych osobowych):*

Upoważnienie
do zarządzania kluczami oraz kodem cyfrowym do systemu alarmowego

Na podstawie Rozdziału 6. Dział 6.3. Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy w Brudzeniu Dużym powierzam Panu/Pani*) .....

zatrudnionemu(nej) na stanowisku .....

w .....

komplet kluczy do budynku Urzędu.

W skład kompletu wchodzą następujące klucze:
1. .....
2. .....
3. .....

Ponadto przydzielam Panu/Pani kod cyfrowy do systemu alarmowego, który należy zachować w ścisłej tajemnicy i wykorzystywać zgodnie z postanowieniami w/w Polityki. *)

miejscowość i data	podpis Administratora

Oświadczam, że przyjmuję pełną odpowiedzialność za powierzone klucze oraz *) kod cyfrowy do systemu alarmowego i zobowiązuję się do ich wykorzystywania jedynie w celach realizacji powierzonych mi zadań zgodnie z niniejszym upoważnieniem.

miejscowość i data	podpis pracownika

*) niepotrzebne skreślić

Wykaz zawartych umów o powierzeniu przetwarzaniu danych osobowych

L.p.	Podmioty, którym Administrator powierzył przetwarzanie danych osobowych	Data zawarcia umowy	Zakres powierzonych do przetwarzania danych osobowych	Okres obowiązywania umowy	Cel zawarcia umowy
1.					
2.					
3.					
...					