

Zarządzenie nr 44/2014
Wójta Gminy Żurawica
z dnia 02 czerwca 2014r.

w sprawie: wprowadzenia Polityki bezpieczeństwa danych osobowych, Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz powołania Administratora Bezpieczeństwa Informacji

Na podstawie: *art. 36 ust.1 i ust.2 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), § 1 i § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100 poz.1024) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 11 grudnia 2008r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji GIODO (Dz. U. z 2008r. Nr 229, poz.1536)* zarządzam, co następuje:

§1.

Wprowadzam w życie Politykę bezpieczeństwa danych osobowych w Urzędzie Gminy Żurawica stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§2.

Wprowadzam w życie Instrukcję zarządzania systemem informatycznym służącą do przetwarzania danych osobowych w Urzędzie Gminy Żurawica stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§3.

Powołuję i zobowiązuję Administratora Bezpieczeństwa Informacji w osobie Pana Adama Miła w Urzędzie Gminy Żurawica do:

- a) prowadzenia nadzoru nad przestrzeganiem i stosowaniem zasad ochrony danych osobowych zgodnie z wymaganiami ustawy o ochronie danych osobowych,
- b) przeprowadzania kontroli zgodności przetwarzania danych osobowych z ustawą o ochronie danych osobowych,
- c) prowadzenia i aktualizacji dokumentacji w ramach ochrony danych osobowych; t.j. Polityki bezpieczeństwa danych osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
- d) sporządzenia i zredagowania klauzul informacyjnych, umów powierzenia przetwarzania danych, oraz innych dokumentów niezbędnych do realizacji zadań zgodnie z wymogami ustawy o ochronie danych osobowych,
- e) przygotowywania i aktualizacji zgłoszeń zbiorów danych osobowych do rejestracji GIODO,
- f) szkoleń pracowników w ramach ochrony danych osobowych,

§4.

Zarządzenie wchodzi w życie z dniem jego podjęcia.


WÓJT
Janusz Szabaga


Załącznik nr 1 do Zarządzenie nr 44/2014
Wójta Gminy Żurawica
z dnia 02 czerwca 2014r.

(Wyłącznie do użytku służbowego)

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

W URZĘDZIE GMINY ŻURAWICA

Żurawica 2014 r.


WÓJT
Janusz Szaboga

Wprowadzenie	3
Rozdział 1	4
Definicje 4	
Rozdział 2	7
Zasady, zakres i wymagania Polityki Bezpieczeństwa Danych Osobowych.....	7
Rozdział 3	8
Odpowiedzialność i organizacja przetwarzania danych osobowych	8
Rozdział 4	12
Procedury tworzenia, rejestrowania i dokonywania zmian w zbiorach danych osobowych.....	12
Rozdział 5	13
Procedury nadawania i cofnięcia upoważnień do przetwarzania danych osobowych	13
Rozdział 6	14
Infrastruktura przetwarzania danych osobowych	14
Rozdział 7	15
Wykaz potencjalnych zdarzeń stanowiących naruszenie ochrony danych osobowych	15
Rozdział 8	16
Zasady postępowania w przypadku naruszenia ochrony danych osobowych	16
Kontrola nad przestrzeganiem zasad ochrony danych osobowych	17
Rozdział 9	18
Zasady przetwarzania danych osobowych powierzonych.....	18
Rozdział 10	19
Postanowienia końcowe	19
Załącznik nr 1	20
UPOWAŻNIENIE	20
Załącznik nr 2	21
OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI	21
Załącznik nr 3	22
WZÓR - EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	22
Załącznik nr 4	23
Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych	23

Wprowadzenie

Polityka Bezpieczeństwa Danych Osobowych wprowadzona jest na podstawie art. 36 ust. 2 w związku z art. 39 a Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz w oparciu o Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

W Urzędzie Gminy Żurawica, zwanym dalej *Urzędem* z uwagi na charakter Instytucji oraz pełnione zadania własne i zlecone z zakresu administracji rządowej przetwarzane są informacje stanowiące dane osobowe w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Niniejszy dokument opisuje zasady postępowania odnoszące się do bezpieczeństwa danych osobowych i został przygotowany z myślą o zapewnieniu standardów bezpieczeństwa przetwarzania danych osobowych w Urzędzie ze szczególnym uwzględnieniem zgodności ich przetwarzania, z obowiązującym prawem zbierania danych dla oznaczonych, zgodnych z prawem celów, oraz zminimalizowania skutków zagrożeń z tytułu utraty poufności, autentyczności danych, strat finansowych, jak również utraty wizerunku placówki.

Urząd podejmuje i realizuje działania w zakresie stosowania odpowiednich standardów bezpieczeństwa danych osobowych oraz wspiera przedsięwzięcia i inicjatywy związane z ich rzeczywistą ochroną i zabezpieczeniem.

Zasadniczym celem Polityki Bezpieczeństwa Danych Osobowych jest przyjęcie, wdrożenie i realizacja działań przy zastosowaniu środków technicznych i organizacyjnych, niezbędnych dla zapewnienia poufności, rozliczalności i integralności przetwarzanych danych dając pełne gwarancje ich ochrony.

Przy opracowaniu niniejszego dokumentu uwzględniono regulacje zawarte w następujących aktach prawnych:

- Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 101, poz. 926 ze zm.),
- Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U.2004 Nr 100, poz.1024),
- Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 11 grudnia 2008r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji GIODO (Dz.U. z 2008r. Nr 229, poz.1536),

Rozdział 1

Definicje

Ilekróć mowa w niniejszym dokumencie o:

1. **Administrator Danych Osobowych** – rozumie się przez to Gminę Żurawica, reprezentowaną przez Wójta Gminy Żurawica, zwanego dalej „Administratorem Danych Osobowych”.
2. **Administrator Bezpieczeństwa Informacji** – rozumie się przez to osobę, której Administrator Danych Osobowych powierzył pełnienie obowiązków Administratora Bezpieczeństwa Informacji, zwany dalej „ABI”.
3. **Administrator Systemu Informatycznego** – rozumie się przez to osobę odpowiedzialną za wdrożenie i stosowanie zasad bezpieczeństwa przetwarzania danych osobowych w zakresie technicznych i programowych zabezpieczeń systemu informatycznego zwany dalej „ASI”.
4. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
5. **Hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych, lub innych, znane jedynie użytkownikowi.
6. **Identyfikator** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
7. **Integralność danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
8. **Osoba upoważniona do przetwarzania danych osobowych** – rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez Administratora Danych Osobowych na piśmie.
9. **Poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.
10. **Przetwarzającym** – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie

danych osobowych na podstawie umowy zawierane zgodnie z art. 31 ustawy.

11. **Raport** – rozumie się przez to przygotowane przez system informatyczny zestawienie zakresu treści przetwarzania danych.
12. **Rozliczalność** – rozumie się przez to właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
13. **Przetwarzanie danych** – jakkolwiek operacja wykonywana na danych osobowych, taka jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza taka, którą wykonuje się w systemach informatycznych.
14. **Ustawa** – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r., Nr 101, poz. 926 ze zm.).
15. **Rozporządzenie** – rozumie się przez to Rozporządzenie Ministra Spraw Wewnętrznych Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz U nr100, poz.1024).
16. **GIODO** – Generalny Inspektor Ochrony Danych Osobowych.
17. **Indywidualne stanowisko komputerowe** – komputer lub inne urządzenie, w którym przetwarzane są dane osobowe, bez podłączenia do sieci Administratora Danych Osobowych.
18. **Informatyczny system przetwarzania** – sposób przetwarzania informacji w systemie informatycznym wraz ze związanymi z nim ludźmi oraz zasobami technicznymi (wykorzystujący technikę cyfrową), który dostarcza i dystrybuuje informacje.
19. **Moduł systemu informatycznego** – element systemu informatycznego, spełniający określone funkcje.
20. **Podmiot zewnętrzny** – osoba fizyczna lub przedsiębiorca wykonujący na rzecz Administratora Danych Osobowych prace zlecone, związane z przetwarzaniem danych osobowych, oraz prace serwisowe urzędów, na których przetwarzane są dane osobowe.
21. **Użytkownik** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło do pracy w systemie informatycznym Administratora Danych Osobowych.

22. **Uwierzytelnienie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
23. **Serwer** – komputer lub zespół komputerów powiązanych ze sobą, będących źródłem informacji i programów dla innych komputerów.
24. **Serwerownia** – wydzielone pomieszczenie z ograniczonym dostępem fizycznym, w którym znajdują się serwery.
25. **Serwisant** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego.
26. **Sieciowe stanowisko komputerowe** – komputer stacjonarny podłączony do sieci komputerowej Administratora Danych Osobowych, w którym przetwarzane są dane osobowe.
27. **Sieć Administratora Danych Osobowych** - sieć łącząca, co najmniej dwa indywidualne stanowiska komputerowe, umożliwiająca określony dostęp do przetwarzania danych upoważnionym użytkownikom.
28. **Sieć publiczna** – rozumie się przez to sieć publiczną w rozumieniu art.2 pkt. 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne.
29. **Sieć telekomunikacyjna** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt. 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U nr 7, poz. 852 ze zm.).
30. **System informatyczny** – oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych stosowanych w celu przetwarzania danych osobowych.
31. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Rozdział 2

Zasady, zakres i wymagania Polityki Bezpieczeństwa Danych Osobowych

1. Zasady oraz wymagania Polityki Bezpieczeństwa Danych Osobowych realizowane są poprzez zapewnienie danym osobowym:
 - a) poufności - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.
 - b) integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione w sposób nieautoryzowany lub nieuprawniony.
 - c) rozliczalności - właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
2. Dla skutecznej realizacji Polityki Bezpieczeństwa Danych Osobowych w Urzędzie zapewnia się:
 - a) stosowanie odpowiednich do zagrożeń i kategorii danych objętych ochroną, środków technicznych i organizacyjnych zapewniających rzeczywiste bezpieczeństwo ich przetwarzania,
 - b) opracowanie i wdrożenie wymaganej przepisami prawa dokumentacji dotyczącej przetwarzania danych osobowych,
 - c) szkolenia pracowników w zakresie ochrony danych osobowych,
 - d) okresowe szacowanie ryzyka zagrożeń dla zbiorów danych osobowych,
 - e) monitorowanie zastosowanych środków ochrony i bezpieczeństwa danych osobowych,

Polityka Bezpieczeństwa Danych Osobowych obowiązuje wszystkich pracowników Urzędu, bez względu na funkcję i pełnione zadania (również stażystów i praktykantów), jednakże w szczególności wiąże pracowników urzędu, którzy mają dostęp do danych osobowych w ramach wypełniania swoich obowiązków służbowych oraz pełnionych zadań przy ich przetwarzaniu.

Zakres stosowania Polityki Bezpieczeństwa Danych Osobowych dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, rejestrach, wykazach, kartach, aktach, dziennikach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych wykorzystywanych do przetwarzania danych osobowych.

Rozdział 3

Odpowiedzialność i organizacja przetwarzania danych osobowych

1. Ochrona danych osobowych przetwarzanych w Urzędzie, dotyczy wszystkich pracowników, mających dostęp do informacji zbieranych, opracowywanych, odczytywanych, oraz przechowywanych tak w formie tradycyjnej, jak i za pomocą systemu informatycznego bez względu na pełnioną funkcję służbową, zajmowane stanowisko, oraz miejsce wykonywania pracy, w tym charakter stosunku pracy.

2. **Administrator Danych Osobowych**, odpowiada za:
Egzekwowanie stosownych działań zgodnie z niniejszą Polityką Bezpieczeństwa Danych Osobowych w celu utrzymania odpowiednich standardów ochrony danych osobowych, a przede wszystkim zapewnienia:
 - a) przetwarzanie danych osobowych zgodnie z obowiązującym prawem,
 - b) podejmowania decyzji o celach i środkach przetwarzania danych osobowych z uwzględnieniem zmian w obowiązującym prawie,
 - c) upoważnienia pracowników do przetwarzania danych osobowych w określonym indywidualnym zakresie, odpowiadającym zakresowi jej obowiązków,
 - d) wyznaczenia Administratora Bezpieczeństwa Informacji nadzorującego zasady ochrony danych osobowych,
 - e) podjęcia odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

3. **Administrator Bezpieczeństwa Informacji (ABI)** odpowiada za:
Realizację postanowień zawartych w niniejszej Polityce Bezpieczeństwa Danych Osobowych oraz postanowień zawartych w Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych:
 - a) nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu zapewnienia poufności i bezpieczeństwa przetwarzania danych osobowych,
 - b) nadzór nad funkcjonowaniem systemu zabezpieczeń w obszarze przetwarzania danych osobowych,
 - c) przeprowadzanie analiz i identyfikacji zagrożeń i ryzyka, na które mogą być narażone procesy przetwarzania danych osobowych oraz pisemne informowanie o wynikach analiz Administratora Danych Osobowych,
 - d) nadzór nad sposobami i zasadami udostępniania danych osobowych odbiorcom danych lub innym podmiotom, opiniowanie umów, których przedmiotem może być powierzenie

- przetwarzania danych podmiotom zewnętrznym,
- e) niezwłoczne informowanie Administratora Danych Osobowych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
 - f) nadzór nad prowadzeniem i aktualizacją dokumentacji z zakresu ochrony danych osobowych,
 - g) inicjowanie szkoleń pracowników z zakresu ochrony danych osobowych i zapoznawanie osób nowo zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,
 - h) nadzór nad wykorzystywanym oprogramowaniem do przetwarzania danych osobowych oraz jego legalnością,
 - i) nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym przeglądaniem pod kątem ich dalszej przydatności.

4. Administrator Systemu Informatycznego odpowiada za:

Realizację zadań w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora Danych Osobowych, w tym zwłaszcza:

- a) zarządza i nadzoruje system informatyczny, w którym przetwarzane są dane osobowe,
- b) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
- c) na wniosek Administratora Danych Osobowych przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także zarządzanie kontami w systemie zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
- d) nadzoruje funkcjonowanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
- e) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
- f) prowadzi dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
- g) sprawuje nadzór nad wykonywaniem napraw, konserwacją lub likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem lub okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
- h) podejmuje działania, służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

5. Osoba upoważniona do przetwarzania danych osobowych:

Zobligowana jest do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych w tym m.in. do:

- a) ochrony danych osobowych przed dostępem osób nieupoważnionych (pracownik nie może pod rygorem odpowiedzialności służbowej i karnej - ujawniać danych, kopiować baz danych oraz przetwarzać danych w sposób inny niż opisany procedurami),
- b) do przetwarzania danych osobowych mogą być dopuszczeni wyłącznie pracownicy posiadający odpowiednie upoważnienie do przetwarzania danych w zakresie ustalonym przez Administratora Danych Osobowych i tylko w celu wykonywania nałożonych na niego obowiązków i zadań. W przypadku przetwarzania danych osobowych w systemie informatycznym zakres dostępu do danych przypisany jest do indywidualnego, niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie informatycznym. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje cofnięcie upoważnienia do przetwarzania danych osobowych,
- c) każdy pracownik, przed dopuszczeniem go do przetwarzania danych musi być zapoznany z przepisami dotyczącymi ochrony danych osobowych oraz niniejszą Polityką Bezpieczeństwa Danych Osobowych i Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych,
- d) pracownik potwierdza zapoznanie się z przepisami dotyczącymi ochrony danych osobowych oraz niniejszą Polityką i Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w stosownym oświadczeniu,
- e) ochrony danych przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją,
- f) zachowania w tajemnicy przetwarzanych danych osobowych, przestrzegania procedur i zasad ich przetwarzania, w tym utrzymywania w tajemnicy powierzonych identyfikatorów, haseł (również w zakresie częstotliwości ich zmiany) – także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji,
- g) stosowania określonych przez Administratora Danych Osobowych procedur oraz zasad mających na celu zgodne z prawem, w tym zwłaszcza adekwatne do celów przetwarzanie danych, oraz nie pozyskiwania jakichkolwiek danych osobowych, przekraczających zakres ustalony czynnościami służbowymi,
- h) korzystania z systemu informatycznego Administratora Danych Osobowych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników,

- i) dbałości o należyte zabezpieczenie wszelkich kartotek, arkuszy, rejestrów, ewidencji, akt, dzienników, kart zawierających dane osobowe, a przede wszystkim chronienia ich przed dostępem do nich osób nieupoważnionych, w tym właściwego przechowywania.

Rozdział 4

Procedury tworzenia, rejestrowania i dokonywania zmian w zbiorach danych osobowych

1. Nadając danym osobowym odpowiednią strukturę, dostępną według określonych kryteriów, niezależnie od tego, czy zestaw jest rozproszony lub podzielony funkcjonalnie – tworzy się zbiory danych osobowych.
2. Każdorazowe tworzenie zbiorów danych osobowych, ich zmiana lub usuwanie musi uzyskać akceptację Administratora Danych Osobowych.
3. Administrator Bezpieczeństwa Informacji prowadzi ewidencję zbiorów danych osobowych oraz rejestruje wszelkie zmiany zachodzące w ich strukturze.
4. Zbiory danych osobowych w Urzędzie tworzy się według następujących zasad:
 - a) nazwa zbioru danych powinna odzwierciedlać cel przetwarzania danych osobowych i być zgodna z nazewnictwem stosowanym w przepisach prawa,
 - b) winna być określona podstawa prawna do przetwarzania danych, lub inna przesłanka prawna legalizująca proces przetwarzania danych osobowych,
 - c) winny być określone środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych w nowo powstałym i zarejestrowanym zbiorze,
5. Administrator Danych Osobowych ma obowiązek zgłosić zbiór danych osobowych do rejestracji w GIODO, z wyjątkiem przypadków określonych w art. 43 ust. 1 Ustawy,
6. Administrator Bezpieczeństwa Informacji przygotowuje zbiór danych osobowych do rejestracji w GIODO zgodnie z wzorem zgłoszenia zbioru danych do rejestracji określonym w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 11 grudnia 2008r.

Rozdział 5

Procedury nadawania i cofnięcia upoważnień do przetwarzania danych osobowych

1. Osoba upoważniona do przetwarzania danych osobowych może przetwarzać dane osobowe wyłącznie w zakresie ustalonym przez Administratora Danych Osobowych w indywidualnym „Upoważnieniu do przetwarzania danych osobowych” i tylko w celu wykonania nałożonych na nią obowiązków.
2. Zakres dostępu do danych osobowych, przetwarzanych w formie papierowej i elektronicznej przypisany jest indywidualnie do każdego pracownika i został określony w imiennym „Upoważnieniu do przetwarzania danych osobowych”.
3. Procedura nadania „Upoważnienia do przetwarzania danych osobowych” dla pracownika zatrudnionego w Urzędzie, przebiega w następujący sposób:

Pracownik ds. kadr w porozumieniu z Administratorem Bezpieczeństwa Informacji:

- a) przygotowuje dla pracownika „Upoważnienie do przetwarzania danych osobowych”, którego wzór stanowi załącznik nr 1 do Polityki Bezpieczeństwa Danych Osobowych oraz „Oświadczenie o zachowaniu poufności”, którego wzór stanowi załącznik nr 2 do Polityki Bezpieczeństwa Danych Osobowych,
 - b) „Upoważnienie do przetwarzania danych osobowych” oraz „Oświadczenie o zachowaniu poufności” przedstawia pracownikowi do podpisu,
 - c) podpisane „Upoważnienie do przetwarzania danych osobowych” oraz „Oświadczenie o zachowaniu poufności” dołączane jest do akt osobowych pracownika.
 - d) wpisuje dane pracownika do „Ewidencji osób upoważnionych do przetwarzania danych osobowych”, której wzór stanowi załącznik nr 3 do Polityki Bezpieczeństwa Danych Osobowych.
4. Pracownik ma *cofane* „Upoważnienie do przetwarzania danych osobowych” w sytuacjach, np.:

-ustania formy zatrudnienia w Urzędzie,

6. Cofnięcie „Upoważnienia do przetwarzania danych osobowych” dla pracownika odbywa się według poniższej procedury:

Pracownik ds. kadr w porozumieniu z Administratorem Bezpieczeństwa Informacji;

- a) przygotowuje wniosek o cofnięcie „Upoważnienia do przetwarzania danych osobowych” dla pracownika lub zmiany zakresu dostępu do przetwarzanych danych osobowych,
-na wniosku wpisuje datę cofnięcia lub zmianę zakresu dostępu, dane identyfikacyjne pracownika oraz ewentualny nowy zakres dostępu do przetwarzanych danych,
 - b) podpisany wniosek dołączany jest do akt osobowych pracownika.
7. Rozwiązanie umowy o pracę powoduje utratę dostępu pracownika do przetwarzania danych osobowych.

Rozdział 6

Infrastruktura przetwarzania danych osobowych

1. Wzór „*Upoważnienia do przetwarzania danych osobowych*” znajduje się w załączniku nr 1 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.
2. Wzór „*Oświadczenia o zachowaniu poufności*” przy przetwarzaniu danych osobowych znajduje się w załączniku nr 2 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.
3. Wzór formularza do prowadzenia „*Ewidencji osób upoważnionych do przetwarzania danych osobowych*” znajduje się w załączniku nr 3 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.
4. W załączniku nr 4 do Polityki Bezpieczeństwa Danych Osobowych znajdują się informacje dotyczące:
 - a) wykazu pomieszczeń, w których dopuszczalne jest przetwarzanie danych osobowych,
 - b) aktualnego wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
 - c) opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązań między nimi,
 - d) opisu sposobu przepływu danych pomiędzy poszczególnymi systemami,
 - e) opisu zabezpieczeń technicznych i organizacyjnych przetwarzanych zbiorów danych osobowych,

Rozdział 7

Wykaz potencjalnych zdarzeń stanowiących naruszenie ochrony danych osobowych

1. Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.
2. Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru.
3. Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu, będący wynikiem nieautoryzowanej modyfikacji danych osobowych.
4. Jakość danych w systemie informatycznym lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie.
5. Naruszenie lub próba naruszenia integralności systemu informatycznego lub bazy danych w tym systemie.
6. Próba lub modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).
7. Ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń.
8. Praca w systemie informatycznym lub jego sieci komputerowej, wykazująca nieprzypadkowe odstępstwa od założonego rytmu pracy, wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
9. Ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki".
10. Podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowanie lub skopiowanie danych osobowych.
11. Naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji.
12. Niewylogowanie się z systemu informatycznego przed opuszczeniem stanowiska pracy.
13. Pozostawienie danych osobowych w drukarce, na ksero.
14. Nie wykonanie w określonym terminie kopii bezpieczeństwa.
15. Prace na danych osobowych w celach prywatnych.
16. Otwarte szafy, biurka, regały, pomieszczenia archiwalne i inne.
17. Nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych.
18. Nieprawidłowości w zakresie zabezpieczenia nośników danych osobowych (wydruków, zdjęć, płyt CD, DVD w formie niezabezpieczonej).

Rozdział 8

Zasady postępowania w przypadku naruszenia ochrony danych osobowych

1. Każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest odpowiedzialny za bezpieczeństwo tych danych, a w sytuacji zauważenia zdarzenia mogącego być przyczyną naruszenia ochrony danych osobowych, zobowiązany jest do niezwłocznego powiadomienia o fakcie Administratora Danych Osobowych lub Administratora Bezpieczeństwa Informacji.
2. Potencjalne przypadki naruszenia ochrony danych osobowych to:
 - a) ślady włamania lub próby włamania do obszaru, w którym przetwarzane są dane osobowe,
 - b) ślady włamania lub próby włamania do pomieszczeń, gdzie odbywa się przetwarzanie danych osobowych, w tym serwerowni oraz pomieszczeń, gdzie przechowywane są nośniki kopii zapasowych oraz szafek, w których przechowywane są w postaci elektronicznej lub papierowej nośniki danych osobowych,
 - c) zagubienie bądź kradzież nośnika danych osobowych,
 - d) kradzież sprzętu informatycznego, w którym przechowywane są dane osobowe,
 - e) informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,
 - f) fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego, przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań lub też działania siły wyższej,
 - g) podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym,
 - h) pojawienie się niestandardowych komunikatów generowanych przez system informatyczny,
 - i) wygląd aplikacji inny niż normalnie,
 - j) brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych,
 - k) spowolnienie działania systemu informatycznego,
 - l) brak możliwości zalogowania się do tej aplikacji.
3. W przypadku wystąpienia któregośkolwiek z powyższych zdarzeń, które zdaniem pracownika mogą wskazywać na zagrożenie bezpieczeństwa danych osobowych, należy niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego.
4. Po otrzymaniu zgłoszenia Administrator Bezpieczeństwa Informacji jest zobowiązany do podjęcia działań w celu:
 - a) wyjaśnienia zdarzenia, w szczególności czy miało miejsce naruszenie ochrony danych osobowych,
 - b) wyjaśnienia przyczyn naruszenia bezpieczeństwa danych osobowych, w szczególności czy

- zdarzenie było związane z celowym działaniem pracownika bądź osób trzecich,
- c) usunięcia skutków zdarzenia,
 - d) przeprowadzenia analizy poprawności funkcjonowania systemu informatycznego, w którym przetwarzane są dane osobowe.
5. W przypadku, gdy incydent był spowodowany celowym działaniem, Administrator Bezpieczeństwa Informacji jest zobowiązany do pisemnego powiadomienia Administratora Danych Osobowych, który może poinformować organy uprawnione do ścigania przestępstw.
6. Administrator Bezpieczeństwa Informacji jest odpowiedzialny za przeprowadzenie przynajmniej raz w roku analizy zaistniałych zdarzeń naruszających bezpieczeństwo danych osobowych w celu określenia potrzeb w zakresie środków technicznych i organizacyjnych podnoszących bezpieczeństwo dla przetwarzanych danych osobowych.

Kontrola nad przestrzeganiem zasad ochrony danych osobowych

1. Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie i dokonuje ich okresowego sprawdzenia.
2. Administrator Bezpieczeństwa Informacji przeprowadza w pierwszym kwartale roku kalendarzowym kontrolę w zakresie przestrzegania przez pracowników zasad i postanowień niniejszej Polityki i Instrukcji Zarządzania Systemem Informatycznym w tym przepisów ustawy o ochronie danych osobowych, z czego sporządza stosowny raport w formie stwierdzonych uchybień, nieprawidłowości i zaleceń pokontrolnych, który przedstawia Administratorowi Danych Osobowych.

Rozdział 9

Zasady przetwarzania danych osobowych powierzonych

1. W przypadku gdy Urząd powierza do przetwarzania dane osobowe innemu podmiotowi odbywa się ono na podstawie umowy zawartej w formie pisemnej.
2. Umowa powinna zawierać ściśle określony cel oraz zakres powierzonych do przetwarzania danych osobowych.
3. Powierzone dane podlegają ochronie na takich samych zasadach jak dane będące własnością Urzędu, chyba że umowa określi inne zasady ochrony danych osobowych.
4. Podmiot któremu powierzono do przetwarzania dane osobowe Urzędu, zobowiązuje się do przestrzegania zasad wskazanych przez Urząd w zawartej umowie oraz przewidzianych w ustawie z dnia 29 kwietnia 1997r. o ochronie danych osobowych, a w szczególności:
 - a) zobowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, przetwarzaniem z naruszeniem ustawy,
 - b) zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do baz danych oraz komu są przekazywane, zwłaszcza, gdy przekazuje się je za pomocą urządzeń teletransmisji danych,
 - c) zapewnić kontrolę nad tym, aby do przetwarzania danych osobowych dopuszczone były wyłącznie osoby posiadające pisemne, imienne upoważnienie do przetwarzania danych osobowych oraz podpisały zobowiązanie do zachowania tajemnicy służbowej,
 - d) zobowiązany do spełnienia warunków technicznych i organizacyjnych, którym powinny odpowiadać urządzenia i systemy informatyczne stosowane przez niego do przetwarzania danych osobowych, tj. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004r., Nr. 100, poz. 1024.).

Rozdział 10

Postanowienia końcowe

1. Administrator Danych Osobowych zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem.
2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego Dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa Informacji lub osoby go zastępującej.
3. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926), Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
4. Niniejsza Polityka Bezpieczeństwa Danych Osobowych wchodzi w życie z dniem jej podpisania przez Administratora Danych Osobowych.



Wojty
Janusz Szaboga

Załącznik nr 1

....., dnia.....

UPOWAŻNIENIE
do przetwarzania danych osobowych nr/2014

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926, z późn. zm.):

upoważniam Pana/Panią

zatrudnionego/ą na stanowisku

w

- do przetwarzania danych osobowych, które obejmuje przetwarzanie danych osobowych w zbiorze:

Lp	Nazwa zbioru danych osobowych	Sposób przetwarzania			
		Z	R	P	W
1					
2					
3					

Sposób przetwarzania:

Użytkownik jest uprawniony do:

Z- zbieranie/opracowanie, (forma papierowa)

R- odczyt/podgląd, (papierowo-elektronicznie)

P- przechowywanie, (papierowo-elektronicznie)

W- wprowadzanie/modyfikacja, (forma elektroniczna)

zgodnie z postanowieniami Polityki Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.

Osoba upoważniona oświadcza, iż zapoznała się z postanowieniami powyżej wskazanych dokumentów.

Osoba upoważniona oświadcza, iż akceptuje treść powyżej wskazanych dokumentów.

.....
(podpis Administratora Bezpieczeństwa Informacji)

.....
(podpis Administratora Danych Osobowych)

Załącznik nr 2

....., dnia

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Imię i nazwisko pracownika;

Stanowisko;

w

Ja niżej podpisany/podpisana* dokumentując dane osobowe zawarte w wszelkich rejestrach, wykazach, arkuszach, dziennikach, itp., na sprzęcie komputerowymprzetwarzającym te dane

zobowiązuję się do:

1. Zapoznania się i przestrzegania przepisów ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2001r Nr 101, poz. 926 z późn. zm.), rozporządzenia Ministra Spraw Wewnętrznych z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100, poz. 1024) oraz uregulowań wewnętrznych tj. Polityki Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym.
2. Zachowania w tajemnicy wszelkich danych osobowych, które uzyskałem/uzyskałam* w związku z zatrudnieniem. Wymogu tego dochowam również po ustaniu zatrudnienia w Urzędzie.
3. Dbłości o należyte zabezpieczenie wszelkich dzienników, kartotek, rejestrów, ewidencji zawierających dane osobowe, a przede wszystkim chronienia ich przed dostępem do nich osób nieupoważnionych.
4. Chronienia wszelkich danych osobowych na wszelkich nośnikach informacji przed ich zniszczeniem, nieuzasadnioną modyfikacją i nielegalnym ich ujawnieniem.
5. Nie pozyskiwania jakichkolwiek danych osobowych przekraczających zakres ustalony czynnościami służbowymi i określony w indywidualnym zakresie obowiązków, uprawnień i odpowiedzialności.
6. Przestrzegania przepisów ustawy z dnia 4 lutego 1994r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006r. Nr 90, poz. 631 z późn. zm.) w części dotyczącej programów komputerowych tzn. wykonywania pracy wyłącznie na programach oficjalnie kupionych i nie instalowania programów pochodzących z innych źródeł ani nie udostępniania programów będących własnością Urzędu. W razie wątpliwości, czy dana aplikacja jest na stanie Urzędu należy zwrócić się do pracownika na stanowisku ds. informatycznych, który określi jego pochodzenie i ewentualnie podejmie kroki w celu całkowitego usunięcia programu z dysku lokalnego. Jednocześnie przyjmuje do wiadomości, że ponoszę odpowiedzialność za bezpieczeństwo danych i programów zainstalowanych na dysku twardym mojego komputera wg posiadanego poziomu dostępu.

Zostałem/zostałam* pouczoney/pouczona, że naruszenie powyższych zobowiązań skutkuje odpowiedzialnością cywilną i karną, wynikającą z tytułu naruszenia w/w ustaw: o ochronie danych osobowych wraz z przepisami wykonawczymi oraz o prawie autorskim i prawach pokrewnych.

* niepotrzebne skreślić

Podpis pracownika

Załącznik nr 3.....
(pieczęć nagłówkowa jednostki organizacyjnej)**WZÓR - EWIDENCJA OSÓB UPOWAŻNIONYCH
DO PRZETWARZANIA DANYCH OSOBOWYCH****W****Administrator Danych Osobowych:**

.....

Administrator Bezpieczeństwa Informacji:

.....

Lp.	Imię i nazwisko (użytkownik)*	Numer upoważnienia	Nazwa identyfikatora (LOGIN)	Data		Uwagi
				nadania uprawnień	ustania uprawnień	
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						

Załącznik nr 4

Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	01
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 18	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
<p style="text-align: center;">Podatek od nieruchomości</p> <p style="text-align: center;">Papierowo - elektronicznie (Forma przetwarzania)</p>		<p style="text-align: center;">Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych</p> <p style="text-align: center;">Program PUMA Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., 85-950 Bydgoszcz, ul. Krupińskiego 9</p>
3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi		
nazwisko i imię, miejsce urodzenia, adres zamieszkania, PESEL, NIP, imiona rodziców, nr KW, powierzchnia budynku, nr działki, powierzchnia gruntu, wartość budowli, nr tel., nr konta bankowego, numer dowodu osobistego, stan cywilny,		
4. Sposób przepływu danych między poszczególnymi systemami		
Wspólna baza danych dla wszystkich aplikacji systemu PUMA, wymiana danych w ramach jednej bazy. Brak przepływu danych pomiędzy różnymi systemami.		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych ; -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - tylko dla użytkowników do aplikacji systemów PUMA) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu PUMA) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji PUMA) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (TAK dla aplikacji PUMA) 		

 Referat Podatków i Oplat
 Inspektor w Referacie Podatków i Oplat

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	02
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 18	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
Rejestr ulg podatkowych Papierowo-elektronicznie (Forma przetwarzania)		Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
		Program PUMA Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., 85-950 Bydgoszcz, ul. Krupińskiego 9 edytor tekstów Word
3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi		
nazwisko i imię, adres zamieszkania, numer aktu notarialnego, dane o gruncie,		
4. Sposób przepływu danych między poszczególnymi systemami		
Wspólna baza danych dla wszystkich aplikacji systemu PUMA, wymiana danych w ramach jednej bazy. Brak przepływu danych pomiędzy różnymi systemami.		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - tylko dla użytkowników do aplikacji systemów PUMA) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu PUMA) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji PUMA) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (TAK dla aplikacji PUMA) 		

 Referat Podatków i Oplat
 Inspektor w Referacie Podatków i Oplat

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	03
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 18	
Referat Podatków i Oplat Inspektor w Referacie Podatków i Oplat	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Podatek rolny	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo - elektronicznie (Forma przetwarzania)	Program PUMA Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., 85-950 Bydgoszcz, ul. Krupińskiego 9
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	nazwisko i imię, miejsce urodzenia, adres zamieszkania, PESEL, NIP, imiona rodziców, nr KW, powierzchnia budynku, nr działki, powierzchnia gruntu, wartość budowli (jeżeli wchodzą prawne) nr tel., nr konta bankowego, numer dowodu osobistego, stan cywilny,	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Wspólna baza danych dla wszystkich aplikacji systemu PUMA, wymiana danych w ramach jednej bazy. Brak przepływu danych pomiędzy różnymi systemami.	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - tylko dla użytkowników do aplikacji systemów PUMA) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu PUMA) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji PUMA) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (TAK dla aplikacji PUMA) 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	04
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 18	
Referat Podatków i Oplat Inspektor w Referacie Podatków i Oplat	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Podatek leśny Papierowo - elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych Program PUMA Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., 85-950 Bydgoszcz, ul. Krupińskiego 9
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	nazwisko i imię, adres zamieszkania, PESEL, NIP, imiona rodziców, nr KW, powierzchnia lasów, nr działki	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Wspólna baza danych dla wszystkich aplikacji systemu PUMA, wymiana danych w ramach jednej bazy. Brak przepływu danych pomiędzy różnymi systemami.	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - tylko dla użytkowników do aplikacji systemów PUMA) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu PUMA) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji PUMA) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (TAK dla aplikacji PUMA) 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	05
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 18	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
Rejestr umorzeń, odroczeń i rozłożeń na raty Papierowo - elektronicznie (Forma przetwarzania)		Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych Program PUMA Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., 85-950 Bydgoszcz, ul. Krupińskiego 9
		3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi
nazwisko i imię, adres zamieszkania, kwota, powód umorzenia, informacje dotyczące stanu zdrowia, miejsce pracy, sytuacja materialna, rodzinna, dochody członków rodziny, wysokość rachunków i opłat, dopłat przynoszone z innych instytucji, zaświadczenia z GOPS		
4. Sposób przepływu danych między poszczególnymi systemami		
Wspólna baza danych dla wszystkich aplikacji systemu PUMA, wymiana danych w ramach jednej bazy. Brak przepływu danych pomiędzy różnymi systemami.		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - tylko dla użytkowników do aplikacji systemów PUMA) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu PUMA) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji PUMA) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (TAK dla aplikacji PUMA) 		

 Referat Podatków i Oplat
 Inspektor w Referacie Podatków i Oplat

Załącznik nr 4

Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	06
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 18	
Referat Podatków i Oplat Podinspektor w Referacie Podatków i Oplat	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Podatek od środków transportowych	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo - elektronicznie (Forma przetwarzania)	Program PUMA Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., 85-950 Bydgoszcz, ul. Krupińskiego 9
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	nazwisko i imię, adres zamieszkania, PESEL, NIP, imiona rodziców, data urodzenia, dane pojazdu, nr dowodu osobistego,	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Wspólna baza danych dla wszystkich aplikacji systemu PUMA, wymiana danych w ramach jednej bazy. Brak przepływu danych pomiędzy różnymi systemami.	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - tylko dla użytkowników do aplikacji systemów PUMA) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu PUMA) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji PUMA) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (TAK dla aplikacji PUMA) 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	07
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: pok. Nr 18	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
Egzekucja należności Papierowo - elektronicznie (Forma przetwarzania)		Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych Program PUMA Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., 85-950 Bydgoszcz, ul. Krupińskiego 9 Moduł Windykacja
3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi		
nazwisko i imię, adres zamieszkania, imiona rodziców, data urodzenia, PESEL, NIP, dane współmałżonka,		
4. Sposób przepływu danych między poszczególnymi systemami		
Wspólna baza danych dla wszystkich aplikacji systemu PUMA, wymiana danych w ramach jednej bazy. Brak przepływu danych pomiędzy różnymi systemami.		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - tylko dla użytkowników do aplikacji systemów PUMA) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu PUMA) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji PUMA) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (TAK dla aplikacji PUMA) 		

**Referat Podatków i Oplat
Podinspektor w Referacie Podatków i Oplat**

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	08
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 18	
Referat Podatków i Oplat Podinspektor w Referacie Podatków i Oplat	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Rejestr zaświadczeń o nie zaleganiu w podatkach i o stanie majątkowym Papierowo-elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
		Program PUMA Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., 85-950 Bydgoszcz, ul. Krupińskiego 9
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	nazwisko i imię, rodzaj zaświadczenia, adres zamieszkania, data wydania, PESEL, NIP, kiedy wpłynął wniosek (data), sposób doręczenia,	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Wspólna baza danych dla wszystkich aplikacji systemu PUMA, wymiana danych w ramach jednej bazy. Brak przepływu danych pomiędzy różnymi systemami.	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - tylko dla użytkowników do aplikacji systemów PUMA) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu PUMA) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji PUMA) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (TAK dla aplikacji PUMA) 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	09
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 18	
Referat Podatków i Oplat Podinspektor w Referacie Podatków i Oplat	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Kwitariusze	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo - elektronicznie (Forma przetwarzania)	Program PUMA Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., 85-950 Bydgoszcz, ul. Krupińskiego 9
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	nazwisko i imię, adres zamieszkania, kwota podatku, nr konta podatkowego	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Wspólna baza danych dla wszystkich aplikacji systemu PUMA, wymiana danych w ramach jednej bazy. Brak przepływu danych pomiędzy różnymi systemami.	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - tylko dla użytkowników do aplikacji systemów PUMA) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu PUMA) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji PUMA) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (TAK dla aplikacji PUMA) 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	10
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II, 37-710 Żurawica Nr pokoju: nr 18	
Referat Podatków i Oplat Podinspektor w Referacie Podatków i Oplat	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Tytuły wykonawcze	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo-elektronicznie (Forma przetwarzania)	Program PUMA Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., 85-950 Bydgoszcz, ul. Krupińskiego 9
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	nazwisko i imię, adres zamieszkania, NIP, PESEL, imiona rodziców, kwota zaległości, termin płatności, odsetki, data urodzenia	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Wspólna baza danych dla wszystkich aplikacji systemu PUMA, wymiana danych w ramach jednej bazy. Brak przepływu danych pomiędzy różnymi systemami.	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych, -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych, -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - tylko dla użytkowników do aplikacji systemów PUMA) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu PUMA) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji PUMA) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (TAK dla aplikacji PUMA) 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	11
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II, 37-710 Żurawica Nr pokoju: nr 18	
Referat Podatków i Oplat Podinspektor w Referacie Podatków i Oplat	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Upomnienia Papierowo-elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych Program PUMA Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., 85-950 Bydgoszcz, ul. Krupińskiego 9
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	nazwisko i imię, adres zamieszkania, kwota zaległości, za jaki okres, NIP	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Wspólna baza danych dla wszystkich aplikacji systemu PUMA, wymiana danych w ramach jednej bazy. Brak przepływu danych pomiędzy różnymi systemami.	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - tylko dla użytkowników do aplikacji systemów PUMA) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu PUMA) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji PUMA) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (TAK dla aplikacji PUMA) 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	12
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 18	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
Zwrot podatku akcyzowego Papierowo - elektronicznie (Forma przetwarzania)		Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
		Arkusz kalkulacyjny Excell
3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi		
nazwisko i imię, adres zamieszkania, nazwa firmy, NIP, PESEL, powierzchnia gruntu, faktury, nr konta bankowego i nazwa banku, seria i nr dowodu osobistego, nr tel., umowy dzierżawy, oświadczenia o użytkowaniu gruntów		
4. Sposób przepływu danych między poszczególnymi systemami		
Nie dotyczy		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 		

Referat Podatków i Oplat
Referent w Referacie Podatków i Oplat

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	13
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II, 37-710 Żurawica Nr pokoju: nr 11	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
Pomoc publiczna Papierowo - elektronicznie (Forma przetwarzania)		Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych programy dostępne SRPP/SHRIMP Arkusze kalkulacyjne Excell
3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi		
nazwisko i imię, wartość pomocy, NIP		
4. Sposób przepływu danych między poszczególnymi systemami		
SHRIMP SRPP → Wnioskodawca		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 		

**Referat Podatków i Oplat
Kierownik w Referacie Podatków i Oplat**

Załącznik nr 4

Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	14
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II, 37-710 Żurawica Nr pokoju: nr 17, 8	
Referat Infrastruktury i Ochrony Środowiska Referent d/s Gospodarki Komunalnej	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	<p style="text-align: center;">Deklaracje dotyczące opłaty za gospodarowanie odpadami komunalnymi</p> <p style="text-align: center;">Papierowo-elektronicznie (Forma przetwarzania)</p>	<p>Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych</p> <p>Program PUMA Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., 85-950 Bydgoszcz, ul. Krupińskiego 9 Moduł Gospodarka Odpadami Komunalnymi</p>
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	imię, nazwisko, adres zamieszkania, PESEL	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Wspólna baza danych dla wszystkich aplikacji systemu PUMA, wymiana danych w ramach jednej bazy. Brak przepływu danych pomiędzy różnymi systemami.	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - tylko dla użytkowników do aplikacji systemów PUMA) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu PUMA) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji PUMA) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (TAK dla aplikacji PUMA) 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	15
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 17, 8	
Referat Infrastruktury i Ochrony Środowiska Referent d/s Gospodarki Komunalnej	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Upomnienia, wezwania i decyzje dotyczące gospodarowania odpadami komunalnymi Papierowo-elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
		Program PUMA Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., 85-950 Bydgoszcz, ul. Krupińskiego 9 Moduł Gospodarka Odpadami Komunalnymi
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	imię, nazwisko, adres zamieszkania	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Wspólna baza danych dla wszystkich aplikacji systemu PUMA, wymiana danych w ramach jednej bazy. Brak przepływu danych pomiędzy różnymi systemami.	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - tylko dla użytkowników do aplikacji systemów PUMA) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu PUMA) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji PUMA) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (TAK dla aplikacji PUMA) 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	16
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 17	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
Decyzje w sprawie odmowy umorzenia opłat za gospodarowanie odpadami		Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
		Edytor tekstów WORD
3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi		
imię, nazwisko, adres zamieszkania,		
4. Sposób przepływu danych między poszczególnymi systemami		
Nie dotyczy		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 		

Referat Infrastruktury i Ochrony Środowiska
Referent d/s Gospodarki Komunalnej

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	17
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 17	
Referat Infrastruktury i Ochrony Środowiska Referent d/s Gospodarki Komunalnej	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Decyzje w sprawie odmowy rozłożenia na raty opłat za gospodarowanie odpadami	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
		Edytor tekstów WORD
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	imię, nazwisko, adres zamieszkania,	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 		

Załącznik nr 4

Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	18
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 17	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
Postanowienie o pozostawieniu podania bez rozpatrzenia		Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
		Edytor tekstów WORD
3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi		
imię, nazwisko, adres zamieszkania,		
4. Sposób przepływu danych między poszczególnymi systemami		
Nie dotyczy		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 		

 Referat Infrastruktury i Ochrony Środowiska
 Referent d/s Gospodarki Komunalnej

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	19
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 17	
Referat Infrastruktury i Ochrony Środowiska Inspektor d/s Ochrony Środowiska	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Ewidencja kodów odpadów segregowanych	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	elektronicznie (Forma przetwarzania)	Plik w arkuszu kalkulacyjnym Excell opracowany na indywidualne zamówienie Urzędu
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	imię, nazwisko, adres zamieszkania, kod paskowy, sposób zagospodarowywania odpadów	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Plik ten jest udostępniany firmie zajmującej się gospodarką odpadami na rzecz gminy.	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	20
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 17	
Referat Infrastruktury i Ochrony Środowiska Inspektor d/s Ochrony Środowiska	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Decyzje środowiskowe Papierowo-elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych Edytor tekstów WORD
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	imię, nazwisko, adres zamieszkania	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 		

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	21
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II, 37-710 Żurawica Nr pokoju: nr 17	
Referat Infrastruktury i Ochrony Środowiska Inspektor d/s Ochrony Środowiska	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Decyzje w zakresie naruszenia stosunków wodnych na gruncie Papierowo-elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
		Edytor tekstów WORD
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	imię, nazwisko, adres zamieszkania	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 	

Załącznik nr 4

Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	22
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 17	
Referat Infrastruktury i Ochrony Środowiska Inspektor d/s Ochrony Środowiska	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Decyzje w zakresie utrzymania czystości i porządku w gminie	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo-elektronicznie (Forma przetwarzania)	Edytor tekstów WORD
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	imię, nazwisko, adres zamieszkania	
	4. Sposób przepływu danych między poszczególnymi systemami	
Nie dotyczy		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 		

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	23
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 19	
Główny Specjalista d/s Dróg i Mostów oraz Budynków i Obiektów Gminnych	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Decyzje o zajęciu pasa drogowego	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo-elektronicznie (Forma przetwarzania)	Edytor tekstów WORD
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwisko, imię, adres zamieszkania	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	24
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 9	
Referat Infrastruktury i Ochrony Środowiska Podinspektor w Referacie	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Beneficjenci programów unijnych elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych plik przesyłany przez Wojewódzki Urząd Pracy - plik PEFS
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	-imię, nazwisko, adres, PESEL, nr telefonu, status na rynku pracy, forma wsparcia jaka uzyskał,	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Dane są przesyłane do Wojewódzkiego Urzędu Pracy	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	25
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 9	
Referat Infrastruktury i Ochrony Środowiska Inspektor d/s Zamówień Publicznych	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Dokumentacja przetargowa zamówień publicznych Papierowo-elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych Edytor tekstów WORD
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwisko, imię, adres siedziby/zamieszkania, NIP, nr telefonu, email,	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Informacja o wyniku postępowania ogłaszana jest na stronie internetowej, tablicy ogłoszeń i publikowana w BIP, Informacja o podpisaniu umowy wysyłana jest do BIP	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 		

Załącznik nr 4

Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	26
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 19	
Główny Specjalista d/s Dróg i Mostów oraz Budynków i Obiektów Gminnych	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Decyzje o zajęciu pasa drogowego Papierowo-elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych Edytor tekstów WORD
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwisko, imię, adres zamieszkania	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	27
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Gminny Ośrodek Pomocy Społecznej, 37-710 Żurawica, ul. Marcina Króla 3	
Samodzielne Stanowisko d/s pomocy osobom uprawnionych do świadczeń z funduszu alimentacyjnego	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Fundusz alimentacyjny	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo - elektronicznie (Forma przetwarzania)	program Nemezis INFO-R Spółka Jawna Kuc Urszula, Kuc Rafał 43-430 Skoczów, ul. Cieszyńska 25
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwisko, imię PESEL, data urodzenia, adres, zadłużenie alimentacyjne, kwota wypłaconych świadczeń, seria i numer dowodu osobistego, imiona rodziców, nazwisko panięskie matki, zawód, numer konta bankowego	
	4. Sposób przepływu danych między poszczególnymi systemami	
lista wypłat trafia do kasy (osoby oddelegowane z GOPS prowadzi to, wypłaty załatwia GOPS) decyzja odnośnie przyznania funduszu trafia do komornika i wierzycielki ale w wersji papierowej informacja o przyznaniu funduszu i wezwanie do podjęcia działań trafia do właściwego ośrodka pomocy społecznej – w wersji papierowej dane dotyczące dłużników nie płacących wpisywane są do Krajowego Rejestru Dłużników poprzez oprogramowanie dostępne w Internecie na stronie KR D		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 		

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	28
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Gminny Ośrodek Pomocy Społecznej, 37-710 Żurawica, ul. Marcina Króla 3	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
<p align="center">Dodatki mieszkaniowe</p> <p align="center">Papierowo - elektronicznie (Forma przetwarzania)</p>		Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
		<p align="center">program CHEOPS INFO-R Spółka Jawna Kuc Urszula, Kuc Rafał 43-430 Skoczów, ul. Cieszyńska 25</p>
3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi		
Nazwisko, imię PESEL, data urodzenia, adres, imiona rodziców, seria i numer dowodu osobistego, numer konta bankowego, nazwisko panięskie matki, kwoty wypłacanych dodatków		
4. Sposób przepływu danych między poszczególnymi systemami		
Lista wypłat w wersji papierowej trafia do kasy GOPS, i w oparciu o nią dokonuje przelewów na konkretne rachunki		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<p>-pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz,</p> <p>-dostęp do klucza od pomieszczenia mają tylko osoby upoważnione,</p> <p>-dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie,</p> <p>-dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania,</p> <p>-pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych ,</p> <p>-prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych ,</p> <p>-pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych,</p> <p>-pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych,</p> <p>-zastosowano oprogramowanie antywirusowe na komputerach użytkowników</p> <p>-zastosowano wygaszacz ekranu + ponowne logowanie</p> <p>-zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania</p> <p>-użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP)</p> <p>-dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników),</p>		

**Samodzielne Stanowisko d/s pomocy osobom
uprawniony do świadczeń z funduszu alimentacyjnego**

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	29
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 16	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
Akta stanu cywilnego Papierowo - elektronicznie (Forma przetwarzania)		Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
		TECHNIKA IT S.A. Ul. Toszecka 2 44-102 Gliwice
3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi		
Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Pesel, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, Nazwisko panieńskie Nazwisko z poprzedniego małżeństwa, Nazwisko rodowe, Miejsce i godzina urodzenia, Data i numer aktu: urodzenia, małżeństwa, zgonu, Imię i nazwisko ojca, matki, współmałżonka, Pleć, Stan cywilny, Data i miejsce zawarcia małżeństwa, Miejsce wystawienia i numer aktu urodzenia żony, Data, godzina, miejsce zgonu, odnalezienia zwłok, Data zgonu męża matki, Nazwisko, imię, adres osoby zgłaszającej zgon, Numer aktu zgonu żony, męża, Nazwisko i nazwisko rodowe małżonka, Nazwisko rodowe matki i ojca mężczyzny, Nazwisko rodowe matki i ojca kobiety, Adnotacje o rozwodzie, Nazwisko po zawarciu małżeństwa:, mężczyzny, kobiety, Data unieważnienia aktu małżeństwa, urodzenia, zgonu, Imię nadane z urzędu Data i numer orzeczenia sądu ustalającego ojcostwo, zaprzeczającego ojcostwo, przysposabiającego dziecko Imię i nazwisko osoby przysposabiającej dziecko, Zmiana nazwiska dziecka, Data rozwiązania poprzedniego małżeństwa, rozwodu		
4. Sposób przepływu danych między poszczególnymi systemami		
Nie dotyczy – praca na jednym stanowisku, na którym znajdują się dane.		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych , -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 		

 USC
 SPRAW OBYWATELSKICH,
 EWIDENCJI DZIAŁALNOŚCI GOSPODARCZEJ,
 BIURO OBSŁUGI KLIENTÓW

Załącznik nr 4

Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	30
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 16	
USC SPRAW OBYWATELSKICH, EWIDENCJI DZIAŁALNOŚCI GOSPODARCZEJ, BIURO OBSŁUGI KLIENTÓW	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Decyzje w sprawie o zmianie imion i nazwisk	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo - elektronicznie (Forma przetwarzania)	Edytor tekstów WORD
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Pesel, seria i numer dowodu osobistego, nazwiska rodziców, imiona małżonka	
4. Sposób przepływu danych między poszczególnymi systemami		
Nie dotyczy		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 		

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	31
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 16	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
<p style="text-align: center;">Medale za długoletnie pozycie małżeńskie</p> <p style="text-align: center;">Papierowo - elektronicznie (Forma przetwarzania)</p>		Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
		Edytor tekstów WORD
3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi		
Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Pesel, seria i numer dowodu osobistego, data ślubu, nazwisko rodowe		
4. Sposób przepływu danych między poszczególnymi systemami		
Nie dotyczy		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<p>-budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe,</p> <p>-budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu,</p> <p>-pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione,</p> <p>-dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie,</p> <p>-dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania,</p> <p>-pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych ,</p> <p>-prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych ,</p> <p>-pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych,</p> <p>-pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych,</p> <p>-zastosowano oprogramowanie antywirusowe na komputerach użytkowników</p> <p>-zastosowano wygaszacz ekranu + ponowne logowanie</p> <p>-zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania</p> <p>-użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP)</p> <p>-dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników),</p>		

 USC
 SPRAW OBYWATELSKICH,
 EWIDENCJI DZIAŁALNOŚCI GOSPODARCZEJ,
 BIURO OBSŁUGI KLIENTÓW

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	32
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 16	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
Działalność gospodarcza Papierowo - elektronicznie (Forma przetwarzania)		Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych program CEDIG
		3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi
Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Pesel, NIP, seria i numer dowodu osobistego, nr. tel., REGON, płeć, dane dotyczące małżeńskiej wspólności majątkowej oraz rachunków bankowych wnioskodawcy, dane osobowe pełnomocnika, nazwisko rodowe osoby składającej wniosek		
4. Sposób przepływu danych między poszczególnymi systemami		
Nie dotyczy		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 		

 USC
 SPRAW OBYWATELSKICH,
 EWIDENCJI DZIAŁALNOŚCI GOSPODARCZEJ,
 BIURO OBSŁUGI KLIENTÓW

Załącznik nr 4

Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	33
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II, 37-710 Żurawica Nr pokoju: nr 16	
USC SPRAW OBYWATELSKICH, EWIDENCJI DZIAŁALNOŚCI GOSPODARCZEJ, BIURO OBSŁUGI KLIENTÓW	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Zbiór danych osobowych PESEL	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo - elektronicznie (Forma przetwarzania)	program PESEL
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Pesel, seria i numer dowodu osobistego, nr. tel., Nazwisko rodowe, nazwiska i imiona poprzednie, nazwiska rodowe rodziców, stan cywilny, nr aktu urodzenia i oznaczenia urzędu stanu cywilnego, który ten akt sporządził, płeć, obywatelstwo, data nabycia obywatelstwa polskiego, imię i nazwisko rodowe małżonka oraz jego nr PESEL, data zawarcia związku małżeńskiego, nr aktu małżeństwa i oznaczenia USC, który ten akt sporządził, data rozwiązania związku małżeńskiego, sygnatura akt i oznaczenie sądu, który rozwiązał małżeństwo, data zgonu małżonka, nr aktu zgonu i oznaczenie USC, który ten akt sporządził, adres i data zameldowania na pobyt stały, poprzednie adresy zameldowania na pobyt stały wraz z określeniem okresu zameldowania, tryb zameldowania na pobyt czasowy trwający ponad 3 miesiące wraz z określeniem okresu zameldowania, tryb wymeldowania, stopień wojskowy, nazwa i seria i nr wojskowego dokumentu osobistego oraz oznaczenie WKU, w której ewidencji osoba pozostaje lub potwierdzenie zgłoszenia się do rejestracji przedpoborowych, serie i numery poprzednich dowodów osobistych oraz daty ich wydania, informacje dot. karty pobytu, zezwolenia na pobyt rezydenta, pobytu tolerowanego, pobytu stałego, statusu uchodźcy, informacje o stałym pobycie członka rodziny obywatela UE, seria i nr tymczasowego zaświadczenia tożsamości cudzoziemca, data jego wydania, data ważności, organ który je wydał.	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	-budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników),	

Załącznik nr 4

Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	34
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 16	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
Ewidencja ludności Papierowo - elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych Program PUMA Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., 85-950 Bydgoszcz, ul. Krupińskiego 9	
3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi		
Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Pesel, seria i numer dowodu osobistego, nazwisko rodowe, imiona i nazwiska poprzednie, nazwiska rodziców, nazwiska rodowe rodziców, stan cywilny, płeć, numer aktu urodzenia, małżeństwa, zgonu wraz z nazwą USC, które akt sporządziło, poprzednie adresy zameldowania na pobyt stały, czasowy, okres zameldowania na pobyt stały, czasowy, obywatelstwo, data zawarcia związku małżeńskiego, data rozwiązania małżeństwa, data zgonu, nazwa wystawcy dowodu osobistego, data wydania oraz data ważności dowodu osobistego, poprzednie dowody osobiste, numery ewidencyjne PESEL rodziców, małżonka, stopień wojskowy, numer dokumentu wojskowego, numer decyzji, data zmiany obywatelstwa		
4. Sposób przepływu danych między poszczególnymi systemami		
Wspólna baza danych dla wszystkich aplikacji systemu PUMA, wymiana danych w ramach jednej bazy. Brak przepływu danych pomiędzy różnymi systemami.		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<p>USC</p> <p>SPRAW OBYWATELSKICH, EWIDENCJI DZIAŁALNOŚCI GOSPODARCZEJ, BIURO OBSŁUGI KLIENTÓW</p> <ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - tylko dla użytkowników do aplikacji systemów PUMA) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu PUMA) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji PUMA) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (TAK dla aplikacji PUMA) 		

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	35
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II, 37-710 Żurawica Nr pokoju: nr 16	
USC SPRAW OBYWATELSKICH, EWIDENCJI DZIAŁALNOŚCI GOSPODARCZEJ, BIURO OBSŁUGI KLIENTÓW	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Dowody osobiste	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo - elektronicznie (Forma przetwarzania)	program MSW
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Pesel, seria i numer dowodu osobistego, nazwisko rodowe, nazwisko rodowe matki, płeć, wzrost w centymetrach, kolor oczu, wizerunek twarzy, adres miejsca pobytu stałego lub czasowego trwającego ponad 3 miesiące,	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	-budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników),	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	35
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II, 37-710 Żurawica Nr pokoju: nr 16	
USC SPRAW OBYWATELSKICH, EWIDENCJI DZIAŁALNOŚCI GOSPODARCZEJ, BIURO OBSŁUGI KLIENTÓW	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Kwalifikacja wojskowa	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo - elektronicznie (Forma przetwarzania)	Program PUMA Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., 85-950 Bydgoszcz, ul. Krupińskiego 9
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, Pesel, seria i numer dowodu osobistego, nazwisko rodowe, seria i numer książeczki wojskowej, kategoria zdolności do służby wojskowej	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Wspólna baza danych dla wszystkich aplikacji systemu PUMA, wymiana danych w ramach jednej bazy. Brak przepływu danych pomiędzy różnymi systemami.	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	-budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - tylko dla użytkowników do aplikacji systemów PUMA) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu PUMA) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji PUMA) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (TAK dla aplikacji PUMA)	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	36
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Gminny Zespół Ekonomiczno-Administracyjny Szkół i placówek Oswaity , 37-710 Żurawica ul. Marcina Króla 3	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
Obowiązek szkolny Papierowo - elektronicznie (Forma przetwarzania)		Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych Edytor tekstów WORD
3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi		
Nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania		
4. Sposób przepływu danych między poszczególnymi systemami		
Nie dotyczy		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
-budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników),		

USC
 SPRAW OBYWATELSKICH,
 EWIDENCJI DZIAŁALNOŚCI GOSPODARCEJ,
 BIURO OBSŁUGI KLIENTÓW

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	37
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 16	
USC SPRAW OBYWATELSKICH, EWIDENCJI DZIAŁALNOŚCI GOSPODARCZEJ, BIURO OBSŁUGI KLIENTÓW	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Zezwolenia na sprzedaż napojów alkoholowych Papierowo (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych -
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, adres zamieszkania, adres punktu sprzedaży	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
-budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych,		

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	38
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 13, 14	
REFERAT ROLNICTWA, GOSPODARKI GRUNTAMI, SPRAW LOKALOWYCH, OBSŁUGI GOSPODARCZEJ URZĘDU	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Sprzedaż nieruchomości	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo - elektronicznie (Forma przetwarzania)	Edytor tekstów WORD
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania, imiona rodziców, nr Pesel, seria i nr. dowodu osobistego, NIP, nr. tel.	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych , -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	39
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 13, 14	
REFERAT ROLNICTWA, GOSPODARKI GRUNTAMI, SPRAW LOKALOWYCH, OBSŁUGI GOSPODARCZEJ URZĘDU	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Sprzedaż, nabycie i zamiana nieruchomości Papierowo - elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych Edytor tekstów WORD
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania, imiona rodziców, nr Pesel, seria i nr. dowodu osobistego, NIP, nr. tel., oznaczenie nieruchomości	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	40
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 13, 14	
REFERAT ROLNICTWA, GOSPODARKI GRUNTAMI, SPRAW LOKALOWYCH, OBSŁUGI GOSPODARCZEJ URZĘDU	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Gospodarka lokalami gminy Papierowo - elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych Edytor tekstów WORD
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, adres zamieszkania, imiona rodziców, seria i nr. dowodu osobistego,	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych , -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	41
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 13	
REFERAT ROLNICTWA, GOSPODARKI GRUNTAMI, SPRAW LOKALOWYCH, OBŚLUGI GOSPODARCZEJ URZĘDU	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Podziały i rozgraniczenia nieruchomości Papierowo - elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych Edytor tekstów WORD
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, adres zamieszkania, imiona rodziców, seria i nr. dowodu osobistego, Pesel	
	4. Sposób przepływu danych między poszczególnymi systemami	
Nie dotyczy		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 		

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	42
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II, 37-710 Żurawica Nr pokoju: nr 14	
REFERAT ROLNICTWA, GOSPODARSTWA GRUNTAMI, SPRAW LOKALOWYCH, OBSŁUGI GOSPODARSTWA URZĘDU	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Decyzje zezwalające na wycinkę drzew Papierowo (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych -
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, adres zamieszkania, informacje dotyczące nieruchomości	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych , -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, 		

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	43
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 13	
REFERAT ROLNICTWA, GOSPODARSTWA GRUNTAMI, SPRAW LOKALOWYCH, OBSŁUGI GOSPODARSTWA URZĘDU	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Numeracja porządkowa nieruchomości Papierowo (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych -
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, adres zamieszkania, informacje dotyczące nieruchomości	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych , -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, 		

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	44
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 13, 14, 18, 8	
REFERAT ROLNICTWA, GOSPODARKI GRUNTAMI, SPRAW LOKALOWYCH, OBSŁUGI GOSPODARCZEJ URZĘDU	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Ewidencja gruntów i budynków Papierowo - elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych Plik SWDE (do podglądu)
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, adres zamieszkania, seria i nr. dowodu osobistego, Pesel, nr ewidencyjny działki, Księga wieczysta	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), 		

Załącznik nr 4

Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	45
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 13	
REFERAT ROLNICTWA, GOSPODARKI GRUNTAMI, SPRAW LOKALOWYCH, OBSŁUGI GOSPODARCZEJ URZĘDU	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Zaświadczenia z planu zagospodarowania przestrzennego	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo-elektroniczne (Forma przetwarzania)	Edytor tekstów WORD
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, adres zamieszkania, nr ewidencyjny działki, obręb ewidencyjny, przeznaczenie działki	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	-budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników),	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	46
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: 15 Pomieszczenie Archiwum	
REFERAT ROLNICTWA, GOSPODARKI GRUNTAMI, SPRAW LOKALOWYCH, OBSŁUGI GOSPODARZEJ URZĘDU	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Archiwum Papierowo (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych -
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Dokumentacja archiwalna	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, 		

Załącznik nr 4

Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	47
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 21	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
Świadczenia osobiste i rzeczowe na rzecz wojska Papierowo (Forma przetwarzania)		Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
		-
3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi		
Nazwiska i imiona, adres zamieszkania, nr tel.		
4. Sposób przepływu danych między poszczególnymi systemami		
Nie dotyczy		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
-budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych,		

**ZESPÓŁ DS.
 OBRONY CYWILNEJ, SPRAW WOJSKOWYCH,
 KULTURY, ZDROWIA,
 KULTURY FIZYCZNEJ I SPORTU,
 KONTAKTÓW Z MEDIAMI, PROMOCJI GMINY**

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	48
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 21	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
ZESPÓŁ DS. OBRONY CYWILNEJ, SPRAW WOJSKOWYCH, KULTURY, ZDROWIA, KULTURY FIZYCZNEJ I SPORTU, KONTAKTÓW Z MEDIAMI, PROMOCJI GMINY	Plany obronne Gminy, obrony cywilnej gminy, zarządzania kryzysowego gminy Papierowo (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych -
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
Nazwiska i imiona, adres zamieszkania, nr tel.		
4. Sposób przepływu danych między poszczególnymi systemami		
Nie dotyczy		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych , -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, 		

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	49
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 7	
ZESPÓŁ DS. OBSŁUGI ORGANÓW GMINY I KADR Stanowisko ds. obsługi organów gminy i kadr urzędu gminy	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Kadry	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo-elektronicznie (Forma przetwarzania)	System Kadry Softers Biuro Usług Komputerowych SOFTRES Sp. z o.o. 35-326 Rzeszów, ul. Zaciszna 44
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	-nazwisko i imię, PESEL, NIP, data i miejsce urodzenia, adres zamieszkania, oświadczenie o niekaralności, kursy i szkolenia, wykształcenie, świadectwa pracy, umowy o pracę, nr telefonu, nr dowodu osobistego, imiona rodziców, nazwisko rodowe, stosunek do służby wojskowej, dane członków, nazwisko i imię, PESEL, adres zamieszkania, zwolnienia lekarskie, skierowania na badania okresowe, ewidencja urlopów, notatki służbowe,	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Wspólna baza dla programu Kadry i Płace, export danych do programu Płatnik (plik w formacie .kdu), export danych do programu księgowego, export danych do programu Home Banking	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	-budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - brak hasła dla użytkowników aplikacji SOFTRES) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu SOFTRES) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji SOFTRES) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (NIE dla aplikacji SOFTRES)	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	50
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 7	
ZESPÓŁ DS. OBSŁUGI ORGANÓW GMINY I KADR Stanowisko ds. obsługi organów gminy i kadr urzędu gminy	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Prace interwencyjne i roboty publiczne	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo (Forma przetwarzania)	-
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, adres zamieszkania, PESEL, NIP, data i miejsce urodzenia, wykształcenie, miejsce pracy, imiona rodziców, data i miejsce urodzenia	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, 		

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	51
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 7	
ZESPÓŁ DS. OBSŁUGI ORGANÓW GMINY I KADR Stanowisko ds. obsługi organów gminy i kadr urzędu gminy	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Staże Papierowo (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych -
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, adres zamieszkania, PESEL, data i miejsce urodzenia, wykształcenie, imiona rodziców, data i miejsce urodzenia	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych l -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	52
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II, 37-710 Żurawica Nr pokoju: nr 7	
ZESPÓŁ DS. OBSŁUGI ORGANÓW GMINY I KADR Stanowisko ds. obsługi organów gminy i kadr urzędu gminy	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Skazani na wykonywanie prac społecznych w Gminie Papierowo (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych -
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, adres zamieszkania, PESEL, data i miejsce urodzenia, imiona rodziców, skazania	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	-budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych , -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych,	

Załącznik nr 4

Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	53
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 11	
ZESPÓŁ DS. OBSŁUGI ORGANÓW GMINY I KADR Stanowisko ds. obsługi organów gminy i kadr urzędu gminy	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Oświadczenia majątkowe radnych Papierowo (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych -
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, adres zamieszkania, PESEL, data i miejsce urodzenia, imiona rodziców, zawód, dane osobowe małżonka, dane dotyczące stanu majątkowego	
	4. Sposób przepływu danych między poszczególnymi systemami Nie dotyczy	
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, 		

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	54
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II, 37-710 Żurawica Nr pokoju: Cały Urząd	
2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
System elektronicznego obiegu dokumentów Papierowo-elektronicznie (Forma przetwarzania)		Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
		SOD SOFTRES Biuro Usług Komputerowych SOFTRES Sp. z o.o. 35-326 Rzeszów, ul. Zacisza 44
3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi		
Nazwiska i imiona, adres zamieszkania, Numer faksu, Adres poczty elektronicznej, Adres www., Rejestr spraw.		
4. Sposób przepływu danych między poszczególnymi systemami		
Dokument trafia do kancelarii, skanowany i dekretowany na stanowisko, dekretuje osoba na biurz podawczym, Dokumenty elektroniczne są drukowane, lub przekazywane bezpośrednio na stanowisko.		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
CAŁY URZĄD	<p>-budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe,</p> <p>-budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu,</p> <p>-pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione,</p> <p>-dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie,</p> <p>-dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania,</p> <p>-pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych,</p> <p>-prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,</p> <p>-pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych,</p> <p>-pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych,</p> <p>-zastosowano oprogramowanie antywirusowe na komputerach użytkowników</p> <p>-zastosowano wygaszacz ekranu + ponowne logowanie</p> <p>-użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP)</p> <p>-dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - brak hasła dla użytkowników aplikacji SOFTRES)</p> <p>-wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu SOFTRES)</p> <p>-zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji SOFTRES)</p> <p>-dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (NIE dla aplikacji SOFTRES)</p>	

Załącznik nr 4

Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	55
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 1 – biuro podawcze	
ZESPÓŁ DS. OBSŁUGI ORGANÓW GMINY I KADR Stanowisko ds. obsługi sekretariatu gminy i spraw kadrowych urzędu gminy	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Korespondencja Papierowo-elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych Poczta elektroniczna
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, adres zamieszkania, adres e-mail	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Nie dotyczy	
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) 		

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	56
1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 1	
ZESPÓŁ DS. OBSŁUGI ORGANÓW GMINY I KADR Stanowisko ds. obsługi sekretariatu gminy i spraw kadrowych urzędu gminy	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Rejestr skarg i wniosków Papierowo (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych -
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwiska i imiona, adres zamieszkania, adres e-mail	
	4. Sposób przepływu danych między poszczególnymi systemami	
Nie dotyczy		
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych - brak aktualnych szkoleń -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych. 		

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	57	
Stanowisko	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
REFERAT KSIĘGOWOŚCI	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 4/5/6/ 10		
	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
	Księgowość budżetowa Papierowo-elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych	
		System Finansowo-księgowy Softers Biuro Usług Komputerowych SOFTRES Sp. z o.o. 35-326 Rzeszów, ul. Zaciszna 44	
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi		
	-nazwisko i imię, PESEL, NIP, adres zamieszkania, nr dowodu osobistego		
	4. Sposób przepływu danych między poszczególnymi systemami		
Import danych z programu Kadry i Płace.			
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych			
<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - brak hasła dla użytkowników aplikacji SOFTRES) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu SOFTRES) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji SOFTRES) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (NIE dla aplikacji SOFTRES) 			

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	58
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 4	
REFERAT KSIĘGOWOŚCI Stanowisko ds. rozliczeń kasowych urzędu	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Kasa – obsługa kasy Urzędu	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo-elektronicznie (Forma przetwarzania)	Program PUMA Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., 85-950 Bydgoszcz, ul. Krupińskiego 9
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	-nazwisko i imię, adres zamieszkania, Pesel, nr dowodu osobistego	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Wspólna baza danych dla wszystkich aplikacji systemu PUMA, wymiana danych w ramach jednej bazy. Brak przepływu danych pomiędzy różnymi systemami.	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych , -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - tylko dla użytkowników do aplikacji systemów PUMA) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu PUMA) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji PUMA) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (TAK dla aplikacji PUMA) 	

Załącznik nr 4

Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	59
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 7/5/6/	
REFERAT KSIĘGOWOŚCI Stanowisko ds. prowadzenia ewidencji księgowej - plac	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Umowy zlecenia, umowy o dzieło	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo-elektronicznie (Forma przetwarzania)	System Placowy Softers Biuro Usług Komputerowych SOFTRES Sp. z o.o. 35-326 Rzeszów, ul. Zacisza 44
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	-nazwisko i imię, adres zamieszkania, seria i numer dowodu osobistego, nr konta bankowego	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Wspólna baza dla programu Kadry i Płace, export danych do programu Płatnik (plik w formacie .kdu), export danych do programu księgowego, export danych do programu Home Banking	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - brak hasła dla użytkowników aplikacji SOFTRES) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu SOFTRES) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji SOFTRES) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (NIE dla aplikacji SOFTRES) 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	60
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II, 37-710 Żurawica Nr pokoju: nr 5	
REFERAT KSIĘGOWOŚCI	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	ZUS	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo-elektronicznie (Forma przetwarzania)	Program Płatnik
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	Nazwisko, imię, PESEL, NIP, data urodzenia, adres zamieszkania, nr dowodu osobistego	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Import danych z Programu Płace i Kadry w postaci pliku (.kdu), export danych do ZUS	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznali się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), -wykonywanie kopii zapasowych (1 raz w tygodniu) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła. 	

Załącznik nr 4

Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	61
	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:	
Stanowisko	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 5	
REFERAT KSIĘGOWOŚCI Stanowisko ds. prowadzenia ewidencji księgowej - płac	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	
	Płace	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych
	Papierowo-elektronicznie (Forma przetwarzania)	Program Płace Softers Biuro Usług Komputerowych SOFTRES Sp. z o.o. 35-326 Rzeszów, ul. Zaciszna 44
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	
	-nazwisko i imię, adres zamieszkania, PESEL, NIP, data i miejsce urodzenia, dane członków rodzin-nr konta bankowego, listy płac pracowników, kartoteki zarobkowe pracowników, nakazy komornicze, angaże, umowy o prace, zastępstwa, zasiłki chorobowe, wychowawcze	
	4. Sposób przepływu danych między poszczególnymi systemami	
	Wspólna baza dla programu Kadry i Płace, export danych do programu Płatnik (plik w formacie .kdu), export danych do programu księgowego, export danych do programu Home Banking	
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	
	<ul style="list-style-type: none"> -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe, -budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu, -pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz, -dostęp do klucza od pomieszczenia mają tylko osoby upoważnione, -dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie, -dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania, -pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych , -prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych , -pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych, -pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych, -zastosowano oprogramowanie antywirusowe na komputerach użytkowników -zastosowano wygaszacz ekranu + ponowne logowanie -użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP) -dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników), aplikacja - brak hasła dla użytkowników aplikacji SOFTRES) -wykonywanie kopii zapasowych (1 raz w tygodniu zarówno dla aplikacji systemu SOFTRES) -zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (Tak dla aplikacji SOFTRES) -dostęp do zbioru danych osobowych zabezpieczony jest za pomocą uwierzytelnienia z wykorzystaniem identyfikatora i hasła - (NIE dla aplikacji SOFTRES) 	

Załącznik nr 4**Opis środków technicznych i organizacyjnych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych**

Urząd Gminy Żurawica	Nr kolejny zbioru, wg rejestru	62	
Stanowisko	1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:		
REFERAT KSIĘGOWOŚCI	Urząd Gminy Żurawica, ul. Ojca Św. Jana Pawła II , 37-710 Żurawica Nr pokoju: nr 5		
	2. Wykaz zbiorów danych osobowych (nazwa zbioru) wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych		
	Przelewy bankowe Papierowo-elektronicznie (Forma przetwarzania)	Nazwa programu komputerowego zastosowanego do przetwarzania zbioru danych osobowych	
		Home banking	
	3. Opis struktury zbioru danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi		
	-nazwisko i imię, adres zamieszkania, nr konta bankowego, kwota		
	4. Sposób przepływu danych między poszczególnymi systemami		
	Import danych z programu Płace i Kadry		
	5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych		
	<p>-budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych spełnia wymagania przeciwpożarowe,</p> <p>-budynek Urzędu Gminy w którym zlokalizowany jest obszar przetwarzania danych osobowych zabezpieczony jest systemem alarmowym/systemem sygnalizacji włamania i napadu,</p> <p>-pomieszczenia w którym zlokalizowany jest obszar przetwarzania danych osobowych zamknięte są na klucz,</p> <p>-dostęp do klucza od pomieszczenia mają tylko osoby upoważnione,</p> <p>-dokumenty w formie papierowej przechowywane w metalowej zamkniętej szafie,</p> <p>-dokumenty po wykorzystaniu są niezwłocznie odkładane do miejsca przechowywania,</p> <p>-pracownicy posiadają imienne upoważnienia do przetwarzania danych osobowych ,</p> <p>-prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych ,</p> <p>-pracownicy zostali przeszkoleni z zakresu ochrony danych osobowych,</p> <p>-pracownicy zapoznani się z postanowieniami Polityki bezpieczeństwa danych osobowych,</p> <p>-zastosowano oprogramowanie antywirusowe na komputerach użytkowników</p> <p>-zastosowano wygaszacz ekranu + ponowne logowanie</p> <p>-zastosowano urządzenie typu UPS chroniące system informatyczny przed skutkami awarii zasilania</p> <p>-użyto system Firewall do ochrony dostępu do sieci komputerowej (PSEAP)</p> <p>-dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (hasło BIOS - brak, hasło do systemu - TAK (ale nie zmieniane - takie same dla wszystkich użytkowników),</p>		

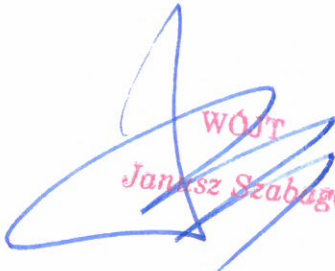
Załącznik nr 2 do Zarządzenie nr 44/2014
Wójta Gminy Żurawica
z dnia 02 czerwca 2014r.

(Wyłącznie do użytku służbowego)

INSTRUKCJA
ZARZĄDZANIA SYSTEMEM
INFORMATYCZNYM
SŁUŻĄCA DO PRZETWARZANIA
DANYCH OSOBOWYCH

w Urzędzie Gminy Żurawica

Żurawica 2014 r.


WÓJTA
Janusz Szabaga

Spis treści

ROZDZIAŁ 1	4
POSTANOWIENIA OGÓLNE.....	4
ROZDZIAŁ 2	7
PROCEDURY NADAWANIA I REJESTROWANIA UPRAWNIENÍ DO PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMIE INFORMATYCZNYM.....	7
ROZDZIAŁ 3	9
METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM.....	9
ROZDZIAŁ 4	12
PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY UŻYTKOWNIKÓW SYSTEMU INFORMATYCZNEGO.	12
ROZDZIAŁ 5	14
PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA.....	14
ROZDZIAŁ 6	16
SPOSOBY, MIEJSCA I OKRESY PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI I WYDRUKÓW ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH.....	16
ROZDZIAŁ 7	18
SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO	18
ROZDZIAŁ 8	21
WYMOGI SYSTEMU W ZAKRESIE PROCEDUR PRZETWARZANIA DANYCH OSOBOWYCH, KONTROLA NAD WPROWADZANIEM, PRZETWARZANIEM I UDOSTĘPNIANIEM DANYCH OSOBOWYCH	21

ROZDZIAŁ 9	25
PROCEDURY WYKONYWANIA PRZEGLĄDÓW, NAPRAW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI, SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	25
ROZDZIAŁ 10	27
POSTĘPOWANIE W PRZYPADKU STWIERDZENIA NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO	27
ROZDZIAŁ 11	29
POSTANOWIENIA KOŃCOWE	29
Załącznik nr 1	31
Załącznik nr 2	32
Załącznik nr 3	34
Załącznik nr 4	37
Załącznik nr 5	38

Rozdział 1

Postanowienia ogólne

§ 1

1. Instrukcja określa ogólne zasady i tryb postępowania Administratora Danych Osobowych w Urzędzie Gminy Żurawica, osób przez niego wskazanych oraz użytkowników przetwarzających dane osobowe w systemie informatycznym, w Urzędzie Gminy Żurawica, zwanym dalej „Urzędem” - w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Instrukcja została opracowana zgodnie z wymogami § 5 **rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).**

§ 2

Użyte w Instrukcji określenia i skróty oznaczają:

1. **Administrator Danych Osobowych** – rozumie się przez to, Gminę Żurawicę zwaną dalej *Gminą* reprezentowaną przez Wójta Gminy Żurawicy, zwanego dalej „Administratorem Danych Osobowych”.
2. **Administrator Bezpieczeństwa Informacji** – rozumie się przez to osobę, której Administrator Danych Osobowych powierzył pełnienie obowiązków Administratora Bezpieczeństwa Informacji, zwany dalej „ABI”.
3. **Administrator Systemu Informatycznego** – rozumie się przez to osobę odpowiedzialną za wdrożenie i stosowanie zasad bezpieczeństwa przetwarzania danych osobowych w zakresie technicznych i programowych zabezpieczeń systemu informatycznego zwany dalej „ASI”.

4. **Dane osobowe**- wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
5. **Hasło**- rozumie się przez to ciąg znaków literowych, cyfrowych, lub innych, znane jedynie użytkownikowi.
6. **Identyfikator**- rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
7. **Integralność danych**- rozumie się przez to właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
8. **Osoba upoważniona do przetwarzania danych osobowych**- rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez Administratora Danych Osobowych na piśmie.
9. **Poufności danych**- rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.
10. **Przetwarzającym**- rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie art. 31 ustawy.
11. **Raport**- rozumie się przez to, przygotowane przez system informatyczny, zestawienie zakresu treści przetwarzania danych.
12. **Rozliczalność**- rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
13. **Przetwarzanie danych**- jakakolwiek operacja wykonywana na danych osobowych, taka jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza taka, którą wykonuje się w systemach informatycznych.
14. **Ustawa**- ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r., Nr 101, poz. 926 ze zm.).
15. **Rozporządzenie**- rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U nr100, poz.1024).
16. **GIODO**- Generalny Inspektor Ochrony Danych Osobowych.
17. **Indywidualne stanowisko komputerowe**- komputer lub inne urządzenie, w którym przetwarzane są dane osobowe, bez podłączenia do sieci Administratora Danych Osobowych.
18. **Informatyczny system przetwarzania**- sposób przetwarzania informacji w systemie informatycznym wraz ze związanymi z nim ludźmi oraz zasobami technicznymi (wykorzystujący

- technikę cyfrową), który dostarcza i dystrybuje informacje.
19. **Moduł systemu informatycznego**- element systemu informatycznego, spełniający określone funkcje.
 20. **Podmiot zewnętrzny**- osoba fizyczna lub przedsiębiorca, wykonująca na rzecz Administratora Danych Osobowych prace zlecone, związane z przetwarzaniem danych osobowych oraz prace serwisowe urzędów, na których przetwarzane są dane osobowe.
 21. **Użytkownik**- rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.
 22. **Uwierzytelnienie**- rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
 23. **Serwer**- komputer lub zespół komputerów powiązanych ze sobą, będących źródłem informacji i programów dla innych komputerów.
 24. **Serwisant**- rozumie się przez to firmę lub pracownika firmy, zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego.
 25. **Sieciowe stanowisko komputerowe**- komputer stacjonarny podłączony do sieci komputerowej Administratora Danych Osobowych, w którym przetwarzane są dane osobowe.
 26. **Sieć Administratora**- sieć, łącząca, co najmniej dwa indywidualne stanowiska komputerowe, umożliwiającą określony dostęp do przetwarzania danych upoważnionym użytkownikom.
 27. **Sieć publiczna**- rozumie się przez to sieć publiczną w rozumieniu art.2 pkt. 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne.
 28. **Sieć telekomunikacyjna**- rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt. 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. nr 7, poz. 852 ze zm.).
 29. **System informatyczny**- oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, stosowanych w celu przetwarzania danych osobowych.
 30. **Zbiór danych**- każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

§ 3

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

Rozdział 2

Procedury nadawania i rejestrowania uprawnień do przetwarzania danych osobowych w systemie informatycznym

§ 4

1. Osoba upoważniona do przetwarzania danych osobowych może przetwarzać dane osobowe wyłącznie w zakresie ustalonym przez, bezpośredniego przełożonego pracownika w indywidualnym upoważnieniu i tylko w celu wykonania nałożonych na nią obowiązków.
2. Zakres dostępu do zbiorów danych osobowych w systemie informatycznym przypisany jest do unikatowego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie informatycznym.

§ 5

Dostęp do systemu informatycznego, służącego do przetwarzania danych osobowych, może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych zarejestrowana, jako użytkownik w tym systemie informatycznym przez Administratora Systemu Informatycznego.

1. W przypadku rejestracji/wyrejestrowania użytkownika w/z systemach/ów informatycznych, nadawanie/odebranie uprawnień przebiega według poniższej procedury:
Bezpośredni przełożony pracownika;
 - a) składa wniosek o nadanie/odebranie uprawnień użytkownika w/z systemie/u informatycznym/ego do Administratora Systemu Informatycznego lub zmiany zakresu dostępu do systemu informatycznego.
 - b) Administrator Systemu Informatycznego dokonuje zmian w systemie informatycznym zgodnie z wnioskiem. W przypadku nadania uprawnień wpisuje na nim identyfikator, datę rejestracji w systemie, a w przypadku wyrejestrowania użytkownika z systemu datę odebrania uprawnień oraz przekazuje podpisany wniosek do ABI.
 - c) Rejestracja użytkownika, o której mowa w pkt. 1, polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.
 - d) ABI wpisuje do Ewidencji osób upoważnionych do przetwarzania danych osobowych nazwę systemu informatycznego oraz identyfikator użytkownika w przypadku jego zarejestrowania w

systemie informatycznym, oraz datę wyrejestrowania użytkownika z systemu informatycznego w przypadku wniosku o jego wyrejestrowanie, następnie po podpisaniu wniosku zwraca go Administratorowi Systemu Informatycznego.

e) Administrator Systemu Informatycznego, w przypadku nadania uprawnień, przekazuje użytkownikowi jego identyfikator i hasło inicjujące pracę w systemie informatycznym oraz przeprowadza szkolenie w zakresie przydzielonych mu obowiązków.

2. Wzór wniosku o nadanie/odebranie uprawnień w systemie informatycznym zawiera załącznik nr 1 do niniejszej Instrukcji.
3. W przypadku zmiany danych identyfikacyjnych, użytkownika, zarejestrowanego w danym systemie informatycznym, obowiązuje następująca procedura:

Bezpośredni przełożony pracownika składa;

- a) wniosek o odebranie uprawnień użytkownika, wpisując na wniosku dane identyfikacyjne, dotyczące użytkownika przed zmianami,
 - b) wniosek o nadanie uprawnień użytkownika w systemie informatycznym wpisując na wniosku aktualne dane identyfikacyjne użytkownika, oraz zakres dostępu do systemu informatycznego.
4. Nadanie/odebranie uprawnień następuje zgodnie z procedurą opisaną w ust. 1.

§ 6

1. Użytkownika wyrejestrowuje się z systemu informatycznego na wniosek bezpośredniego przełożonego pracownika, w sytuacjach:
 - a) ustania zatrudnienia użytkownika w Urzędzie,
 - b) zmiany zakresu obowiązków służbowych lub stanowiska pracy użytkownika.
2. Rozwiązanie umowy o pracę powoduje utratę dostępu użytkownika do przetwarzania danych.
3. Bezpośredni przełożony zobowiązany jest w sytuacjach, o których mowa w ust. 1 i 2 do niezwłocznego przekazywania wniosków o odebranie uprawnień w systemie informatycznym do Administratora Systemu Informatycznego.

Rozdział 3

Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 7

System informatyczny, w którym przetwarza się dane osobowe, wyposażony jest w mechanizmy uwierzytelnienia użytkowników oraz kontroli dostępu.

Identyfikator

1. Identyfikator użytkownika składa się, z co najmniej czterech znaków, z których, np. dwa pierwsze odpowiadają dwóm pierwszym literom imienia użytkownika, a dwa kolejne – dwóm pierwszym literom jego nazwiska.
2. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika, Administrator Systemu Informatycznego, za zgodą Administratora Bezpieczeństwa Informacji, nadaje inny identyfikator, odstępując od zasady określonej w pkt. 1.
3. Identyfikator, po wyrejestrowaniu osoby z systemu informatycznego, nie może być przydzielony innej osobie.
4. Używanie identyfikatorów należących do innych osób jest zabronione.
5. Kontrolę nad powyższymi czynnościami, sprawuje Administrator Systemu Informatycznego.

Hasło użytkownika

1. Hasło dostępu składa się z unikalnego zestawu, co najmniej ośmiu znaków, zawierać ma małe i wielkie litery oraz cyfry i znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani z jego imieniem lub nazwiskiem.
2. W systemie informatycznym zmiana haseł dostępu winna następować regularnie, co 30 dni zgodnie rozporządzeniem.
3. Hasła dostępu wyświetlane są na ekranie monitora w formie niedającej się odczytać osobom postronnym i muszą być znane tylko użytkownikowi.
4. Hasło dostępu, ustala dla siebie użytkownik. Za zmianę hasła odpowiada użytkownik.
5. Zabrania się użytkownikom systemu udostępniania swojego hasła innym osobom oraz korzystania

przez osoby upoważnione do przetwarzania danych osobowych z innego hasła innego użytkownika.

6. Zabrania się tworzenia haseł na podstawie:
 - o sekwencji klawiszy klawiatury
 - o identyfikatora użytkownika
 - o innych haseł łatwych do odgadnięcia
7. W przypadku, gdy użytkownik otrzymuje hasło początkowe (tymczasowe, jednorazowe) od Administratora Systemu Informatycznego, ma obowiązek zmienić je przy pierwszym logowaniu do systemu informatycznego.
8. Użytkownik niezwłocznie zmienia hasło w przypadku podejrzenia lub stwierdzenia:
 - a) podglądu,
 - b) przechwycenia,
 - c) podsłuchania,
 - d) odgadnięcia.

Hasło administratora/ów

1. Hasła Administratora/ów Systemu Informatycznego przechowywane są w postaci klasycznego zapisu w zabezpieczonej kopercie lub na elektronicznych nośnikach informacji CD-ROM – jednokrotnego zapisu, w postaci odpowiednio zabezpieczonego pojedynczego pliku.
2. Hasła, o których mowa w ust. 1, przechowuje się w zamkniętej metalowej szafie, lub sejfie ognioodpornym.
3. W sytuacjach awaryjnych lub w razie nieobecności Administratora Systemu Informatycznego jego zadania spoczywają na osobach upoważnionych przez Administratora Danych Osobowych. W przypadku wykorzystania haseł podczas nieobecności Administratora Systemu Informatycznego muszą być one niezwłocznie zmienione po wznowieniu wykonywania obowiązków.

§ 8

1. Użytkownik zobowiązany jest do utrzymania hasła dostępu w tajemnicy (tak w czasie zatrudnienia, jak też po jego ustaniu).
2. W sytuacji udostępnienia hasła innej osobie, jego faktyczny właściciel ponosi odpowiedzialność za skutki i następstwa wynikłe z faktu wykorzystania tego hasła przez osoby trzecie.
3. Użytkownik nie może przechowywać hasła w formie jakiegokolwiek rodzaju zapisu, w tym w postaci makra, przypisania do klawiszy funkcyjnych lub jakiegokolwiek zautomatyzowanego

procesu rejestracji w systemie informatycznym.

4. W przypadku zastosowania awaryjnego dostępu do systemu informatycznego na poziomie użytkownika (zapomniane hasło, blokada dostępu). Administrator Systemu Informatycznego nadpisuje hasło użytkownika za pomocą nowego hasła początkowego, po dokonaniu uprzedniej weryfikacji tożsamości użytkownika.

Rozdział 4

Procedury rozpoczęcia, zawieszenia i zakończenia pracy użytkowników systemu informatycznego.

§ 9

1. Użytkownik rozpoczynający pracę, zobowiązany jest przestrzegać procedury mającej na celu sprawdzenie zabezpieczeń systemu, a w szczególności:
 - a) sprawdzenie zabezpieczeń fizycznych pomieszczenia,
 - b) sprawdzenie ogólnego stanu sprzętu informatycznego oraz miejsca przechowywania nośników zawierających dane osobowe.
2. Rozpoczęcie pracy na stacji roboczej następuje po włączeniu zasilacza awaryjnego (UPS) i komputera, a następnie wprowadzeniu indywidualnego, znanego tylko użytkownikowi oraz hasła, mając na uwadze, iż:
 - a) po przekroczeniu określonej liczby prób logowania, system informatyczny blokuje dostęp do zbioru danych na poziomie użytkownika. Użytkownik powinien poinformować o tym zdarzeniu Administratora Systemu Informatycznego, który podejmuje stosowne w tym zakresie czynności.
3. Użytkownik, w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym, w czasie pracy ma obowiązek:
 - a) ustawienia monitorów w pomieszczeniach, w sposób uniemożliwiający osobom nieupoważnionym podgląd, a w przypadku przetwarzania danych sensytywnych, jeżeli jest to możliwe, stosowania monitorów z ekranami wyposażonymi w filtry, uniemożliwiające obserwację zawartości ekranu z pozycji innej niż na wprost monitora,
 - b) zapewnienia, aby w obszarach przetwarzania danych osobowych, osoby nieupoważnione do przetwarzania danych nie przebywały bez nadzoru osoby upoważnionej do przetwarzania danych,
 - c) stosowania wygaszacza ekranu w czasie zawieszenia przetwarzania danych (przerwa w pracy). Wyłączenie wygaszacza należy zabezpieczyć hasłem znanym tylko użytkownikowi,
 - d) wylogowania się z systemu w przypadku, kiedy przerwa w pracy trwa dłużej niż 30 minut,
 - e) nie pozostawiania bez nadzoru (np. w drukarce lub na biurku) nośników informacji (np. wydruków dokumentów lub dyskietek), zawierających dane osobowe – dotyczy to także okresu po zakończeniu pracy (obowiązuje tzw. zasada „czystego biurka” i „czystego ekranu”).

4. Logowanie się oraz praca na innych stanowiskach, niż indywidualne stanowisko komputerowe użytkownika, wymaga zgody przełożonego i jest dozwolone jedynie w sytuacjach wyjątkowych lub związanych z pracą zmianową.
5. Przed zakończeniem pracy w systemie informatycznym, użytkownik zobowiązany jest wykonać następujące czynności:
 - a) zapisać wszelkie zmiany w otwartych aplikacjach,
 - b) wykonać kopie zapasowe, jeżeli jest to przewidziane w dokumentacji systemu,
 - c) zamknąć wszystkie używane programy,
 - d) sprawdzić, czy w urządzeniach nie pozostały wymienne elektroniczne nośniki informacji,
 - e) zamknąć system poprzez użycie polecenia „Zamknij system”.
6. Po zakończeniu pracy w systemie informatycznym użytkownik zobowiązany jest przestrzegać następującej procedury:
 - a) wylogować się z systemu i poczekać na jego wyłączenie,
 - b) sprawdzić, czy elektroniczne nośniki informacji, zawierające dane osobowe, nie zostały pozostawione bez nadzoru,
 - c) wyłączyć odbiorniki energii elektrycznej, zamknąć i zabezpieczyć pomieszczenie, jeżeli wychodzi, jako osoba ostatnia,
 - d) umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,
 - e) opuszczając pokój, należy zamknąć za sobą drzwi na klucz.
7. Użytkownik zobowiązany jest do postępowania zgodnie z obowiązującymi procedurami, instrukcjami i podręcznikami, dotyczącymi administrowania, eksploatacji i użytkowania systemu informatycznego, służącego do przetwarzania danych osobowych oraz stosowania się do zaleceń Administratora Systemu Informatycznego i Administratora Bezpieczeństwa Informacji.

Rozdział 5

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

§ 10

1. W celu zapewnienia bezpieczeństwa w systemie informatycznym, przetwarzającym dane osobowe, istnieje obowiązek tworzenia kopii zapasowych.
2. Dostęp do kopii bezpieczeństwa mają tylko osoby upoważnione przez Administratora Danych Osobowych.
3. Kopie zapasowe przeznaczone są do odtworzenia zbioru danych lub systemu, w przypadku całkowitej lub częściowej zmiany, utraty, uszkodzenia czy też zniszczenia zbioru danych bądź systemu.
4. Nośniki, zawierające kopie bezpieczeństwa, należy opisać, zarejestrować i przechowywać odpowiednio zabezpieczone.

§ 11

1. Wyboru metody i częstotliwości tworzenia kopii zapasowych, nośnika do ich zapisywania, dokonuje Administrator Systemu Informatycznego, po uzgodnieniu z Administratorem bezpieczeństwa informacji, uwzględniając specyfikę systemów i zbiorów danych oraz tempo ich narastania.
2. Kopie zapasowe poszczególnych aplikacji, zainstalowanych na stacjach roboczych, wykonywane są za pomocą specjalistycznego oprogramowania archiwizującego dane.
3. Kopie zapasowe:
 - a) programów i narzędzi – wykonuje właściwy Administrator Systemu Informatycznego.
4. Sprawdzenie kopii bezpieczeństwa pod kątem ich dalszej przydatności do odtworzenia danych w wypadku awarii systemu, dokonuje Administrator Systemu Informatycznego.
5. Po upływie przydatności lub okresu przechowywania kopii zapasowych, podlegają one nadpisaniu nową kopią zapasową.

6. Kopie zapasowe, które zostały przeznaczone do likwidacji, pozbawia się zapisu danych osobowych poprzez nadpisanie danych lub ich fizyczne zniszczenie.
7. Uszkodzone kopie zapasowe, dyski lub inne elektroniczne nośniki informacji, które zawierają dane osobowe, należy niszczyć mechanicznie, w sposób uniemożliwiający ich ponowne użycie.
8. Czynności, o których mowa w ust. 6 i 7, wykonuje Administrator Systemu Informatycznego w obecności powołanej komisji przez ABI. Z wykonanych czynności sporządza się protokół, którego kopię przechowuje ABI.
9. Wzór protokołu, o którym mowa w ust. 8, stanowi załącznik nr 4 do niniejszej Instrukcji.

Rozdział 6

Sposoby, miejsca i okresy przechowywania elektronicznych nośników informacji i wydruków zawierających dane osobowe oraz kopii zapasowych

§ 12

1. Czas przechowywania kopii zapasowych powinien być nie krótszy niż jest to konieczne dla bezpieczeństwa systemu informatycznego.

§ 13

1. W celu zapewnienia bezpieczeństwa kopii zapasowych należy przechowywać je w innych pomieszczeniach, niż centra przetwarzania danych osobowych.
2. Nośniki informacji, zawierające dane osobowe, przechowuje się w zamkniętych na klucz szafach, zabezpieczonych meblach biurowych, lub specjalnych do tego typu zastosowań szafach na nośniki magnetyczne.
3. Pomieszczenia i sprzęty, o których mowa w ust. 1 i 2, powinny zapewniać bezpieczeństwo przechowywania kopii zapasowych i elektronicznych nośników informacji, zawierających dane osobowe, przed nieuprawnionym dostępem, modyfikacją, uszkodzeniem lub ich zniszczeniem.

§ 14

1. Nośniki informacji, zawierające dane osobowe, można przekazywać do innej jednostki organizacyjnej tylko na pisemny, umotywowany wniosek, gdy jest to bezwzględnie konieczne do realizacji jej zadań regulaminowych.
2. Nośniki informacji, o których mowa w ust. 1, trzeba na czas transportu odpowiednio zabezpieczyć przed dostępem osób nieuprawnionych.
3. Zakazuje się przetwarzania danych osobowych na nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną bez uprzedniego zaszyfrowania ich w konsultacji z administratorem systemu informatycznego.

4. W przypadku posługiwania się nośnikami danych, pochodzącymi od podmiotu zewnętrznego, użytkownik zobowiązany jest do sprawdzenia go programem antywirusowym na wyznaczonym w tym celu stanowisku komputerowym.
5. Nośniki magnetyczne z zaszyfrowanymi danymi osobowymi są na czas ich użyteczności przechowywane w zamkniętych na klucz szafkach, a po wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki te są niszczone.
6. Dokumenty oraz wydruki, zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie. Za bezpieczeństwo dokumentów odpowiedzialne są osoby je przetwarzające oraz kierownicy właściwych komórek organizacyjnych, odpowiedzialni są za:
 - a) zamykanie dokumentów na klucz w szafkach biurowych, sejfach podczas nieobecności w pomieszczeniach lub po zakończeniu pracy;
 - b) niszczenie dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania;
 - c) niepozostawienie wydruków i ksero na urządzeniach bez nadzoru.

Rozdział 7

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

§ 15

1. Obszarami systemu informatycznego narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są m. in.:
 - a) dysk twardy urządzenia,
 - b) pamięć RAM,
 - c) elektroniczne nośniki informacji np. płyty CD /DVD, pamięci USB,
2. Drogą przedostania się wirusów i szkodliwego oprogramowania do systemu mogą być sieci informatyczne, zainfekowane elektroniczne nośniki danych, oraz załączniki poczty e-mail, pochodzące od nieznanymi nadawców.
3. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu specjalistycznego oprogramowania antywirusowego, zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez Administratora Systemu Informatycznego.
4. Systemy antywirusowe sprawują ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami.
5. W przypadku zastosowania oprogramowania antywirusowego na lokalnej stacji roboczej, nie zarządzanej przez serwer antywirusowy, użytkownik ma obowiązek na bieżąco sprawdzać obecność wirusów w systemie. Opcja automatycznego rozpoznawania i sygnalizowania obecności wirusów powinna być elementem systemu i uaktywniać się w momencie jego uruchomienia.
6. Użytkownik zobowiązany jest powiadomić Administratora Systemu Informatycznego o wykryciu wirusa, niemożliwego do usunięcia przez program antywirusowy chyba, że system informatyczny wyposażony jest w centralny system antywirusowy z centralną kontrolą zarządzania.
7. Do obowiązków Administratora Systemu Informatycznego należy aktualizacja oprogramowania antywirusowego. W przypadku systemów antywirusowych z opcją automatycznej aktualizacji, obowiązki Administratora Systemu Informatycznego ograniczają się do sprawdzenia poprawności

wykonania aktualizacji przez system. W przypadku błędnie wykonanej aktualizacji baz antywirusowych, Administrator Systemu Informatycznego ma obowiązek dokonania ręcznej aktualizacji.

§ 16

1. Administrator Systemu Informatycznego jest zobowiązany zabezpieczyć system przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do danych, poprzez wdrażanie technicznych i logicznych zabezpieczeń chroniących system. Podejmuje również działania:
 - a) kontroli przepływu informacji pomiędzy wewnętrznym systemem informatycznym i publiczną siecią informatyczną oraz kontroli działań inicjowanych z sieci informatycznej i systemu,
 - b) zastosowania systemu Firewall do ochrony dostępu do sieci komputerowej,
 - c) zabezpieczenia sieci bezprzewodowej
 - d) instalowania w systemie oprogramowania zapobiegającego nieuprawnionemu dostępowi do danych osobowych,
 - e) zastosowanie mechanizmów monitorujących przeglądanie Internetu przez użytkowników (blokowanie stron internetowych określonego typu, analiza przesyłanych informacji pod kątem niebezpiecznego oprogramowania,
 - f) nadzór i opiekę techniczną nad systemem poczty elektronicznej:

§ 17

1. Urządzenia i nośniki, zawierające dane osobowe, które są przekazywane poza obszar przetwarzania, zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez hasło dostępu.
2. W przypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych należy zastosować szczególnie środki bezpieczeństwa, które obejmują:
 - a) zastosowanie mechanizmów szyfrowania danych osobowych,
 - b) zastosowanie mechanizmów podpisu elektronicznego, zabezpieczającego transmisje danych osobowych oraz rejestrację transmisji wysyłanych danych osobowych.

3. Umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.

Rozdział 8

Wymogi systemu w zakresie procedur przetwarzania danych osobowych, kontrola nad wprowadzaniem, przetwarzaniem i udostępnianiem danych osobowych

§ 18

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system powinien zapewniać odnotowanie:
 - a) daty pierwszego wprowadzenia danych do systemu;
 - b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu chyba, że dostęp do
 - c) systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
 - d) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
 - e) informacji o odbiorcach, w rozumieniu art. 7 pkt. 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba, że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
 - f) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt. 8 ustawy.

§ 19

1. Odnotowanie informacji, o których mowa w ust. 1 pkt. a i b, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
2. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.
3. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt. 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§ 20

1. Urządzenia i elektroniczne nośniki informacji, zawierające dane wrażliwe, przekazywane poza obszar przetwarzania tych danych, obowiązkowo zabezpiecza się przed:
 - a) dostępem osób i podmiotów nieupoważnionych,
 - b) modyfikacją, lub zniszczeniem w sposób nieautoryzowany.

§ 21

1. Osoba użytkująca komputer przenośny lub inne urządzenie, zawierające dane osobowe, zobowiązana jest do zachowania szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem.

Użytkownik komputera przenośnego jest zobowiązany do:

- transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia;
 - przenoszenie komputera w bagażu podręcznym;
 - nie pozostawienie komputera w samochodzie, hotelu, przechowalni bagażu, w miejscach publicznych itp.,
- zabezpieczenia komputera przenośnego hasłem,
- blokowanie dostępu komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez pracownika,
- wykorzystywanie haseł odpowiedniej, jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym, przetwarzającym dane osobowe,
- nie zezwala osobom nieupoważnionym do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe,
- kopiowanie danych osobowych przetwarzanych na komputerze przenośnym do systemu informatycznego, w celu umożliwienia wykonywania kopii awaryjnych tych danych,
- korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera przenośnego w miejscach publicznych i w środkach transportu publicznego,
- zapewnienia stosowania środków ochrony kryptograficznej podczas transmisji danych z komputerów przenośnych oraz dodatkowo zastosować oprogramowanie do szyfrowania dysków twardych.

§ 22

1. Uwzględniając kategorie przetwarzanych danych osobowych oraz fakt podłączenia do sieci publicznej, Administrator Systemu Informatycznego zobowiązany jest do zastosowania w systemie środków bezpieczeństwa, określonych w załączniku do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
2. Wyróżnia się 3 poziomy bezpieczeństwa zbiorów przetwarzanych przy użyciu systemów informatycznych:
 - a) podstawowy, – gdy w systemie nie są przetwarzane dane wrażliwe i żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych, nie jest połączone z siecią publiczną
 - b) podwyższony, – gdy w systemie są przetwarzane dane wrażliwe i żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych, nie jest połączone z siecią publiczną
 - c) wysoki, – gdy chociaż jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, jest połączone z siecią publiczną

§ 23

Zarządzania dostępem do poczty elektronicznej

Konto pocztowe

1. W Urzędzie Gminy mogą występować dwa rodzaje elektronicznych kont pocztowych:
 - a) Indywidualne (przypisane do osoby, np. Jana Kowalskiego)
 - b) Funkcyjne (przypisane do zadania, np. działalności sekretariatu)
2. Nazwa konta indywidualnego tworzona jest wg reguły:
[pierwsza litera imienia][nazwisko]@zurawica.pl

UWAGA: w nazwie nie stosuje się polskich znaków diaktrycznych (zostają zamienione wg reguły: ń→n)

3. W przypadku ewentualnego dublowania nazw skrzynki przy stosowaniu ww. reguły należy nowotworzoną skrzynkę uzupełnić o kolejną literę imienia. Przy wyczerpaniu tej metody należy zastosować indeksy cyfrowe (np. w Urzędzie pracuje 2-ch Janów Kowalskich, więc zgodnie z podaną zasadą utworzone zostaną konta: j.kowalski@zurawica.pl oraz ja.kowalski@zurawica.pl)
4. Nazwa konta funkcyjnego tworzona jest wg reguły:
5. [nazwa]@zurawica.pl, gdzie nazwą może być np. „sekretariat”.

UWAGA: w nazwie nie stosuje się polskich znaków diaktrycznych (zostają zamienione wg reguły: ń→n)

6. Konto funkcyjne przypisane jest do konkretnej osoby (określonej we wniosku o utworzenie kont podstawowych użytkownika).
7. W przypadku nieobecności tej osoby i konieczności zapewnienia dostępu do konta funkcyjnego, kierujący komórką organizacyjną w dyspozycji którego znajduje się ww. konto realizuje wniosek o utworzenie kont podstawowych użytkownika, zmieniając właściciela skrzynki (opcja „Zmiana właściciela funkcyjnego konta pocztowego”);
8. Standardowy rozmiar konta pocztowego to 100 Mb. Potrzebę zwiększenia rozmiaru skrzynki wraz z uzasadnieniem należy przedstawić we Wniosku o nadanie uprawnień podstawowych użytkownika, w polu: „Szczegółowy, umotywowany opis uprawnień w systemie, jeżeli inny niż standardowy”

Rozdział 9

Procedury wykonywania przeglądów, napraw i konserwacji systemów oraz nośników informacji, służących do przetwarzania danych osobowych.

§ 24

1. Wykonywanie przeglądów i konserwacja systemu informatycznego ma na celu:
 - a) przegląd stosowanych elementów bezpieczeństwa,
 - b) kontrolowanie właściwej konfiguracji systemu,
 - c) sprawdzenie funkcjonalności i jakości pracy systemu,
 - d) zakwalifikowanie sprzętu i urządzeń do naprawy lub modyfikacji.
2. Zakres czynności, o których mowa w ust. 1 pkt. a, obejmuje w szczególności:
 - a) sprawdzenie działania urządzeń zabezpieczających przed nieuprawnionym dostępem,
 - b) kontrolę działania awaryjnego zasilania,
 - c) kontrolę czasu uaktywnienia wygaszaczy ekranu oraz sposobu ich zabezpieczenia,
 - d) sprawdzenie poprawności wykonania kopii bezpieczeństwa.
3. Zakres czynności, o których mowa w ust. 1 pkt. b i c, obejmuje:
 - a) sprawdzenie poprawności zainstalowanych aplikacji oraz urządzeń,
 - b) inwentaryzację zainstalowanego oprogramowania, służącego do przetwarzania danych osobowych,
 - c) kontrolę działania zabezpieczeń systemowych w „Dzienniku Zdarzeń”.

§ 25

1. Przegląd i konserwację systemu wykonują:
 - a) Administrator Systemu Informatycznego,
 - b) podmioty zewnętrzne, uprawnione przez Administratora Danych Osobowych lub osobę przez niego upoważnioną do wykonywania naprawy i konserwacji, w obszarze przetwarzania danych osobowych, na podstawie zawartej umowy,
 - c) podmioty zewnętrzne, w ramach usług serwisowych, na podstawie zawartej umowy.

2. Administrator Systemu Informatycznego pozbawia zapisu danych urządzenia, dyski lub inne elektroniczne nośniki informacji, przekazane do naprawy podmiotowi, o którym mowa w ust. 1 pkt. c.
3. Napraw i konserwacji, o których mowa w ust. 1 pkt. b, dokonuje się pod nadzorem Administratora Systemu Informatycznego lub osoby upoważnionej przez Administratora Danych Osobowych.
4. Administrator Systemu Informatycznego ma obowiązek niezwłocznie powiadomić ABI o działaniach, o których mowa w ust. 1 pkt. b i c.
5. Wykaz podmiotów, o których mowa w ust. 1, pkt. b i c, prowadzi ABI, którego wzór stanowi załącznik nr 5 do niniejszej Instrukcji.

Rozdział 10

Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego.

§ 26

1. Stałą kontrolę bezpieczeństwa przetwarzania danych osobowych na swoim stanowisku pracy, sprawuje użytkownik.
2. Użytkownik zobowiązany jest do zwracania uwagi i zgłaszania do ABI wszelkich zauważonych lub podejrzewanych słabości systemów i usług oraz zagrożeń z nimi związanych.
3. Przypadki podejmowania przez użytkowników wszelkich działań - niezgodnych z ich zakresem obowiązków i obowiązującymi instrukcjami - dotyczących sprzętu, i oprogramowania uznaje się, jako naruszenie bezpieczeństwa danych osobowych.

§ 27

1. Naruszeniem bezpieczeństwa danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub zniszczenia danych lub jakiegokolwiek elementu systemu informatycznego lub nieinformatycznego niezbędnego do przetwarzania danych.
2. Za naruszenie bezpieczeństwa danych osobowych uważa się w szczególności:
 - a) udostępnienie lub umożliwienie zapoznania się z danymi osobowymi osobom nieupoważnionym,
 - b) zmiany w narzędziach programowych lub sprzętowych, powodujące naruszenie ich integralności,
 - c) kradzież lub zniszczenie nośników informacji, zawierających dane osobowe,
 - d) złamanie zabezpieczeń, umożliwiające wykonanie czynności wymienionych w ust. 1,
 - e) jakąkolwiek nieupoważnioną ingerencję w przetwarzane dane.

§ 28

1. W przypadku stwierdzenia okoliczności wskazujących na naruszenia bezpieczeństwa danych osobowych, o których mowa w § 14 ust. 2, użytkownik zobowiązany jest do bezzwłocznego powiadomienia bezpośredniego przełożonego, który powiadamia ABI,
2. ABI ma obowiązek, po rozpoznaniu sprawy sporządzić raport z przebiegu zdarzenia, którego wzór stanowi załącznik nr 2 do niniejszej Instrukcji.
3. Do czasu przybycia ABI, użytkownik zobowiązany jest do:
 - a) powstrzymania się od pracy na urządzeniach, w których zaistniało naruszenie systemu bezpieczeństwa, jak również uruchamiania urządzeń, które mogą mieć związek z zaistniałym zdarzeniem,
 - b) zanotowania wszelkich możliwych informacji związanych ze zdarzeniem, a w szczególności komunikatów, pojawiających się na ekranie,
 - c) podjęcia, stosownie do zaistniałej sytuacji działań, które zapobiegą ewentualnej utracie danych osobowych,
 - d) fizycznego odłączenia komputera od sieci informatycznej (w uzasadnionych przypadkach).
4. ABI, po otrzymaniu informacji o naruszeniu bezpieczeństwa systemu informatycznego, zleca Administratorowi Systemu Informatycznego podjęcie działań zmierzających do wyjaśnienia przyczyn powstania zagrożenia, oceny negatywnych skutków oraz do ich usunięcia.

§ 29

1. ABI w przypadku stwierdzenia:
 - a) złego stanu urządzenia lub niewłaściwego działania programu – niezwłocznie informuje Administratora Systemu Informatycznego, który zleca wykonanie czynności serwisowych oraz sporządza dla ABI notatkę wyjaśniającą przyczyny zaistniałej sytuacji,
 - b) naruszenia przez użytkownika obowiązków pracowniczych w zakresie danych osobowych albo zdarzenia posiadającego znamiona przestępstwa (np. włamanie do sieci) – bezzwłocznie informuje bezpośredniego przełożonego danego użytkownika.
1. W celu realizacji zadań związanych z ochroną danych osobowych, ABI, ma prawo żądania pisemnych wyjaśnień od pracowników, informując o powyższym fakcie Administratora Danych Osobowych.
2. Wykaz form naruszeń bezpieczeństwa przetwarzania danych osobowych stanowi załącznik nr 3 do niniejszej Instrukcji.

Rozdział 11

Postanowienia końcowe

§ 30

Użytkownikom, korzystającym z systemu informatycznego, zabrania się instalowania na komputerach jakiegokolwiek oprogramowania, jeżeli nie są do tego uprawnieni.

§ 31

Użytkownik dopuszczony do korzystania z systemu informatycznego musi być przeszkolony przez Administratora Systemu Informatycznego w zakresie inicjowania pracy komputerów pracujących w sieci oraz postępowania w wypadku wykrycia awarii lub wystąpienia nietypowych zdarzeń.

§ 32

1. ABI prowadzi okresową kontrolę przestrzegania zasad ochrony danych osobowych w Urzędzie.

§ 33

1. Dane osobowe, przekazane do przetwarzania innemu podmiotowi, na podstawie umowy, mogą być przetwarzane tylko w zakresie i celu określonym w umowie.
2. Odpowiedzialność za przestrzeganie procedur, dotyczących bezpieczeństwa danych powierzonych innemu podmiotowi, o których mowa w ust. 1, spoczywa na Administratorze Danych Osobowych lub osobie przez niego upoważnionej oraz podmiocie, z którym zawarto umowę.

§ 34

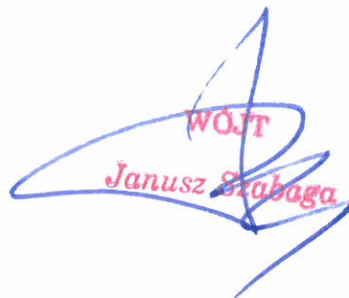
1. Pracownicy są odpowiedzialni za przestrzeganie procedur przetwarzania danych osobowych, określonych przez Administratora Danych Osobowych.
2. Naruszenie przez pracownika, posiadającego upoważnienie do przetwarzania danych osobowych postanowień niniejszej Instrukcji, może stanowić podstawę do pociągnięcia go do odpowiedzialności, z tytułu naruszenia obowiązków pracowniczych.

§ 35

Administrator Systemu Informatycznego lub inne osoby, upoważnione przez Administratora Danych Osobowych, zobowiązani są do uwzględniania warunków bezpieczeństwa danych osobowych przy wprowadzeniu rozwiązań programowych i sprzętowych, służących do przetwarzania danych.

§ 36

W sprawach nieuregulowanych niniejszą Instrukcją mają zastosowanie przepisy ustawy o ochronie danych osobowych oraz odrębne akty, regulaminy dotyczące bezpieczeństwa teleinformatycznego.


WOJT
Janusz Szabaga

Załącznik nr 1 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Wniosek o nadanie/odebranie * uprawnień w Systemie Informatycznym		Nr:
1. Imię i nazwisko.....		
2. Stanowisko		
3. Jednostka organizacyjna:.....		
4. Komórka organizacyjna:.....		
1. Nazwa systemu:.....		
2. Rodzaj uprawnień:		
..... /podgląd, modyfikacja, administrowanie/*		
A. Uzasadnienie wniosku:		
.....		
.....		
.....		
/data/		/podpis i pieczętka/
Potwierdzam nadanie/odebranie* uprawnień dla użytkownika o identyfikatorze:		
.....		
/data/		/podpis i pieczętka/
Potwierdzam wpisanie danych do ewidencji.		
.....		
/data/		/podpis i pieczętka/

* niepotrzebne skreślić

Załącznik nr 2 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.**Raport o naruszeniu ochrony danych osobowych****Sporządzający raport:**

Imię i nazwisko:

Jednostka organizacyjna:

Stanowisko (funkcja):

Dział:

Adres, pokój, nr tel.:

Forma/y naruszenia bezpieczeństwa przetwarzania danych osobowych:

1. Miejsce, dokładny czas i data naruszenia ochrony danych osobowych (jednostka organizacyjna, data, godzina, piętro, nr pokoju, itp.):

2. Osoby powodujące naruszenie, (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia ochrony danych osobowych):

3. Osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych:

4. Informacje o danych, które zostały lub mogły zostać ujawnione:

5. Zabezpieczone materiały lub inne dowody związane z wydarzeniem:

6. Krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania):

	<i>Osoby uczestniczące w zdarzeniu (Nazwisko, imię, podpis, data)</i>	<i>Administrator Bezpieczeństwa Informacji (Nazwisko, imię, podpis, data)</i>	<i>Administrator Systemu Informatycznego (Nazwisko, imię, podpis, data)</i>
1)			
2)			

Załącznik nr 3 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

**Wykaz form naruszeń bezpieczeństwa przetwarzania danych osobowych
w systemie informatycznym:**

Formy naruszenia bezpieczeństwa ochrony danych osobowych przez pracowników zatrudnionych przy przetwarzaniu danych osobowych w systemie informatycznym	
A.	
w zakresie wiedzy	
A1	Ujawnianie sposobu działania aplikacji
A2	Ujawnienie systemu zabezpieczeń osobom niepowołanym
A3	Inne
B.	
w zakresie sprzętu i oprogramowania	
B1	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do danych
B2	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do danych przez jakiegokolwiek inne osoby niż osoba, której identyfikator został przydzielony
B3	Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do aplikacji służącej do przetwarzania danych
B4	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do danych przez osoby nieupoważnione
B5	Modyfikowanie parametrów systemu i aplikacji przez osoby do tego nieupoważnione
B6	Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym
B7	Inne
C.	
w zakresie dokumentów i obrazów zawierających dane osobowe	
C1	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru
C2	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych
C3	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie
C4	Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią

C5	Dopuszczenie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe
C6	Sporządzanie kopii danych na nośnikach danych w sytuacjach nieprzewidzianych procedurą
C7	Utrata kontroli nad kopią danych
C8	Inne
D.	
w zakresie infrastruktury i pomieszczeń stanowiących obszar przetwarzania danych osobowych	
D1	Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych, co stwarza ryzyko dokonania w sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych
D2	Dopuszczanie do kontaktu ze sprzętem komputerowym osób nieupoważnionych
D3	Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiegokolwiek urządzenia do sieci informatycznej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji
D4	Inne
E.	
w zakresie pomieszczeń, w których znajdują się komputery centralne i urządzenia sieci	
E1	Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.)
E3	Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych lub ignorowania takiego faktu
E4	Inne
F.	
zjawiska świadczące o możliwości naruszenia bezpieczeństwa przetwarzania danych osobowych	
F1	Ślady manipulacji przy układach sieci komputerowej lub komputerach
F2	Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu
F3	Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych
F4	Nieoczekiwane nie dające się wyjaśnić zmiany zawartości zbiorów danych
F5	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania

F6	Ślady włamania do pomieszczeń, w których przetwarzane są dane
F7	Inne
G	
formy naruszenia bezpieczeństwa przetwarzania danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem	
G1	Próba uzyskania hasła uprawniającego do dostępu do danych w ramach pomocy technicznej
G2	Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika
G3	Inne

Załącznik nr 4 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

PROTOKÓŁ LIKWIDACJI KOPII ZAPASOWYCH NR.....

Sporządzający raport: Administrator Systemu Informatycznego ABI

IMIĘ I NAZWISKO:

Jednostka organizacyjna: _____
Stanowisko: _____
Komórka organizacyjna: _____
Adres, nr pokoju, nr tel.: _____

Data likwidacji kopii zapasowych:

Miejsce likwidacji kopii zapasowych (miasto, ulica, _____
budynek, piętro, nr pomieszczenia): _____

L.p.	Rodzaj nośnika	Nazwa nośnika	Nr seryjny lub inwentaryzacyjny	Sposób zniszczenia (Informatyczny/Mechaniczny)
1.				
2.				
3.				
4.				
5.				

**Administrator
Systemu Informatycznego**

**Administrator Bezpieczeństwa
Informacji**

Data i podpis

Data i podpis

Załącznik nr 5 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

**WYKAZ PODMIOTÓW UPRAWNIONYCH PRZEZ ADMINISTRATORA DO WYKONYWANIA
NAPRAWY I KONSERWACJI SYSTEMU W OBSZARZE PRZETWARZANIA DANYCH**

Lp.	Nr umowy	Jednostka organizacyjna PP	Podmiot			Pracownicy podmiotu		
			Nazwa	Miasto, Adres	NIP	Imię	Nazwisko	Nr upoważnienia wydanego przez Administradora