WÓJT GMINY FRYSZTAK
ul. Ks. Wojciecha Blajera 20
38-130 Frysztak
woj. podkarpackie
tel. (17) 27 77 110, fax (17) 27 77 920

Zarządzenie Nr III/337/2014

Wójta gminy Frysztak

z dnia 25 listopada 2014 roku

w sprawie wprowadzenia „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Frysztak".

Działając na podstawie § 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) oraz § 95 ust.2 Statutu Gminy Frysztak

zarządza się co następuje

§ 1

Wprowadza się „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Frysztak" zwaną dalej „Instrukcją", która stanowi załącznik zarządzenia.

§ 2

Zobowiązuje się pracowników Urzędu Gminy Frysztak do stosowania zasad określonych w Instrukcji

§ 3

Wykonanie zarządzenia powierza sie administratorowi Systemu Informacji.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr inż. Jan Ziarnik

RADCA PRAWNY
mgr Jerzy Koczot

Załącznik do zarządzenia Nr III/337/2014
Wójta Gminy Frysztak z dnia 25.11.2014 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCA DO PRZETWARZANIA DANYCH OSOBOWYCH

w Urzędzie Gminy we Frysztaku

SPIS TREŚCI

1. Wprowadzenie

1. Instrukcja Zarządzania Systemem Informatycznym służy do określenia ogólnych zasad i trybu postępowania podczas przetwarzania danych osobowych w systemie informatycznym Urzędu Gminy we Frysztaku, w celu zminimalizowania incydentów mogących doprowadzić do uzyskania dostępu do danych osobowych przez osoby nieupoważnione, nieautoryzowaną zmianą, lub zniszczeniem danych.
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).**
3. Użyte w Instrukcji określenia i skróty oznaczają:

L.p.	Skrót/Nazwa	Opis
1.	**Przetwarzanie danych**	operacje wykonywane na danych osobowych, odczytywanie, zapisywanie, modyfikacja, usuwanie, przechowywanie, udostępnianie.
2.	**ADO (Administrator Danych Osobowych)**	Urząd Gminy Frysztak reprezentowany przez Wójta Gminy Frysztak, który decyduje o celach i środkach przetwarzania danych osobowych, sprawuje władztwo nad przetwarzaniem danych osobowych.
3.	**ABI (Administrator Bezpieczeństwa Informacji)**	Osoba, która została upoważniona przez ADO do nadzorowania, przestrzegania oraz stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną.
4.	**ASI (Administrator Systemu Informatycznego)**	osoba odpowiedzialna za stosowanie zasad polityki bezpieczeństwa podczas przetwarzania danych osobowych oraz ich właściwe zabezpieczenie w systemach informatycznych.
5.	**Dane osobowe**	wszelkie informacje umożliwiające zidentyfikowanej osoby fizycznej.
6.	**Integralność danych**	informacja mówiąca o tym, że dane osobowe nie zostały zmienione lub usunięte w sposób nieautoryzowany.
7.	**Poufność danych**	zapewnienie, że dane nie zostały udostępnione lub ujawnione osobom lub systemom nieupoważnionym.
8.	**Rozliczalność**	zapewnienie, że działanie dowolnego podmiotu podczas przetwarzania danych może być jednoznacznie przypisane temu podmiotowi.
9.	**Pracownik**	należy przez to rozumieć osobę zatrudnioną na podstawie umowy o pracę lub umowy cywilno-prawnej, oraz osoby odbywającej staż w Urzędzie Gminy.

10.	**Użytkownik**	osoba upoważniona do przetwarzania danych osobowych, przez ADO lub ABI, identyfikująca się w systemie własnym hasłem i identyfikatorem.
11.	**Identyfikator**	ciąg znaków identyfikujący użytkownika w systemie informatycznym, z pomocą którego można jednoznacznie rozliczyć operacji wykonane przez użytkownika.
12.	**Hasło**	ciąg znaków znany jedynie użytkownikowi, umożliwiający uwierzytelnienie się w systemie informatycznym.
13.	**System informatyczny**	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji stosowanych w celu przetwarzania danych osobowych.
14.	**Sieć telekomunikacyjna**	rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt. 23 ustawy z dnia 21 lipca2 2000 r. – Prawo telekomunikacyjne (Dz U nr 7, poz. 852 ze zm.).
15.	**Sieć publiczna**	rozumie się przez to sieć publiczną w rozumieniu art.2 pkt. 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne.
16.	**Ustawa**	Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r., Nr 101, poz. 926 ze zm.).
17.	**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).
18.	**GIODO**	Generalny Inspektor Ochrony Danych Osobowych
19.	**Serwer**	Komputer lub zespół komputerów powiązanych ze sobą, udostępniających informacje dla systemów informatycznych.
20.	**Serwisant**	Firma lub pracownik firmy zajmujący się instalacja, naprawą, konserwacją systemów informatycznych.

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

1. Osoba upoważniona do przetwarzania danych osobowych może przetwarzać dane osobowe wyłącznie w zakresie ustalonym przez Administratora Danych Osobowych, w indywidualnym upoważnieniu i tylko w celu wykonania nałożonych na nią obowiązków.
2. Zakres dostępu do danych osobowych w systemie informatycznym przypisany jest do unikatowego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie informatycznym.
3. Procedura upoważniania do przetwarzania danych osobowych pracownika zatrudnionego w Urzędzie Gminy we Frysztaku przebiega w następujący sposób:

Administrator Danych Osobowych w porozumieniu z Referentem ds. osobowych oraz Administratorem Bezpieczeństwa Informacji:

1. przygotowuje dla pracownika **Upoważnienie**, którego wzór stanowi załącznik nr 3 do **Polityki Bezpieczeństwa Danych Osobowych** oraz **Oświadczenie**, którego wzór stanowi załącznik nr 4 do **Polityki Bezpieczeństwa Danych Osobowych,**
2. Upoważnienie oraz Oświadczenie przedstawia pracownikowi do podpisu,
3. podpisane Upoważnienie oraz Oświadczenie włącza do akt osobowych pracownika,
4. Wpisuje dane pracownika do **Rejestru osób upoważnionych do przetwarzania danych osobowych**, której wzór stanowi załącznik nr 5 do **Polityki Bezpieczeństwa Danych Osobowych.**

Dostęp do systemu informatycznego, służącego do przetwarzania danych osobowych, może uzyskać wyłącznie osoba upoważniona przez Administratora 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:

Administrator Danych Osobowych lub upoważniona przez niego osoba, jaką jest Referent ds. osobowych w porozumieniu z Administratorem Bezpieczeństwa Informacji;

1. składa wniosek o nadanie/odebranie uprawnień użytkownika w/z systemie/u informatycznym/ego do Administratora Systemu Informatycznego lub zmiany zakresu dostępu do systemu informatycznego.
2. 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 sytemu datę odebrania uprawnień oraz przekazuje podpisany wniosek do ABI.
3. Rejestracja użytkownika, o której mowa w pkt. 1, polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

Administrator Danych Osobowych, lub upoważniona przez niego osoba jaką jest Referent ds. osobowych, 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.

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

Administrator Danych Osobowych lub upoważniona przez niego osoba jaką jest Referent ds. osobowych w porozumieniu z Administratorem Bezpieczeństwa Informacji;

1. Przygotowuje wniosek o odebranie uprawnień użytkownika, wpisując na wniosku dane identyfikacyjne, dotyczące użytkownika przed zmianami,
2. Przygotowuje wniosek o nadanie uprawnień użytkownika w systemie informatycznym wpisując na wniosku aktualne dane identyfikacyjne użytkownika, oraz zakres dostępu do systemu informatycznego.

5. Nadanie/odebranie uprawnień następuje zgodnie z procedurą opisaną w ust. 1.

1. Użytkownika wyrejestrowuje się z systemu informatycznego na wniosek Administratora Danych Osobowych w sytuacjach:

1. ustania zatrudnienia pracownika
2. zmiany zakresu obowiązków służbowych lub stanowiska pracy pracownika.
3. Rozwiązanie umowy o pracę powoduje utratę dostępu użytkownika do przetwarzania danych.
4. Administrator Danych Osobowych lub upoważniona przez niego osoba jaką jest Referent ds. osobowych 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.

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

System informatyczny, w którym przetwarza się dane osobowe, powinien być wyposażony 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 z 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:
   - sekwencji klawiszy klawiatury
   - identyfikatora użytkownika
   - 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.
9. Użytkownik zobowiązany jest do utrzymania hasła dostępu w tajemnicy (tak w czasie zatrudnienia, jak też po jego ustaniu).
10. W sytuacji udostępnienia hasła innej osobie, jego faktyczny właściciel ponosi odpowiedzialność za skutki i następstwa wynikłe z faktu wykorzystania tego hasła przez osoby trzecie.
11. Do weryfikacji tożsamości użytkowników w systemie informatycznym, można stosować inne niż hasło metody uwierzytelniania, w tym karty mikroprocesorowe lub metody biometryczne.
12. 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.
13. 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.

4. Procedury rozpoczęcia, zawieszenia i zakończenia pracy użytkowników systemu informatycznego

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 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 zaczekać 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.

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

1. W celu zapewnienia bezpieczeństwa w systemie informatycznym, przetwarzającym dane osobowe, istnieje obowiązek tworzenia kopii zapasowych.
2. W systemie informatycznym wykorzystującym technologie klient-serwer kopie zapasowe wykonuje się po stronie serwera.
3. Dostęp do kopii bezpieczeństwa mają tylko osoby upoważnione przez Administratora Danych Osbowych.
4. 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.
5. Nośniki, zawierające kopie bezpieczeństwa, należy opisać, zarejestrować i przechowywać odpowiednio zabezpieczone.
6. Wyboru metody i częstotliwości tworzenia kopii zapasowych, nośnika do ich zapisywania, dokonuje Administrator Systemu Informatycznego, po uzgodnieniu z Administratorem Danych Osobowych, uwzględniając specyfikę systemów i zbiorów danych oraz tempo ich narastania.
7. Kopie zapasowe poszczególnych aplikacji, zainstalowanych na stacjach roboczych, wykonywane są za pomocą specjalistycznego oprogramowania archiwizującego dane.
8. Kopie zapasowe:
   a) na serwerze – wykonuje właściwy Administrator Systemu Informatycznego,
   b) Programów i narzędzi- wykonuje właściwy Administrator Systemu Informatycznego.
9. Sprawdzenie kopii bezpieczeństwa pod kątem ich dalszej przydatności do odtworzenia danych w wypadku awarii systemu, dokonuje Administrator Systemu Informatycznego.
10. Po upływie przydatności lub okresu przechowywania kopii zapasowych, podlegają one nadpisaniu nową kopią zapasową.
11. Kopie zapasowe, które zostały przeznaczone do likwidacji, pozbawia się zapisu danych osobowych poprzez nadpisanie danych lub ich fizyczne zniszczenie.
12. Uszkodzone kopie zapasowe, dyski lub inne elektroniczne nośniki informacji, które zawierają dane osobowe, należy niszczyć mechanicznie, w sposób uniemożliwiający ich ponowne użycie.
13. 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.

14. Wzór protokółu, o którym mowa w ust. 8, stanowi załącznik nr 4 do niniejszej Instrukcji.

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

1. Czas przechowywania kopii zapasowych powinien być nie krótszy niż jest to konieczne dla bezpieczeństwa systemu informatycznego.
2. W celu zapewnienia bezpieczeństwa kopii zapasowych należy przechowywać je w innych pomieszczeniach, niż centra przetwarzania danych osobowych.
3. 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.
4. 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.
5. 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.
6. Nośniki informacji, o których mowa w ust. 1, trzeba na czas transportu odpowiednio zabezpieczyć przed dostępem osób nieuprawnionych.
7. 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.
8. 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.
9. 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.

7. Sposób zabezpieczenia systemu informatycznego przed działalnością programowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

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 nieznanych 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.
8. 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) instalowanie w systemie oprogramowania zapobiegającego nieuprawnionemu dostępowi do danych osobowych.

9. 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.
10. 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.
11. Umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.

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

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 ten 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.
2. Odnotowanie informacji, o których mowa w ust. 1 pkt. a i b, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system powinien zapewniać sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.
4. 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.
5. 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.
6. 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.
7. Użytkownik komputera przenośnego jest zobowiązany do:
   - transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia;
   - przenoszenie komputera w bagażu podręcznym;

- nie pozostawianie 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.

8. 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).
9. 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

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

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".
4. 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.
5. 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.
6. 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.
7. Administrator Systemu Informatycznego ma obowiązek niezwłocznie powiadomić ABI o działaniach, o których mowa w ust. 1 pkt. b i c.
8. Wykaz podmiotów, o których mowa w ust. 1, pkt. b i c, prowadzi ABI, którego wzór stanowi załącznik nr 5 do niniejszej Instrukcji.

10. Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

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.
4. 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.
5. 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.
6. 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,
7. ABI ma obowiązek, po rozpoznaniu sprawy sporządzić raport z przebiegu zdarzenia, którego wzór stanowi załącznik nr 2 do niniejszej Instrukcji.
8. 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 zapobiegną ewentualnej utracie danych osobowych,

d) fizycznego odłączenia komputera od sieci informatycznej (w uzasadnionych przypadkach).

9. 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.
10. 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.
11. W celu realizacji zadań związanych z ochroną danych osobowych, ABI, ma prawo żądania pisemnych wyjaśnień od pracowników, informując o powyższym fakcie Administratora Danych Osobowych.
12. Wykaz form naruszeń bezpieczeństwa przetwarzania danych osobowych stanowi załącznik nr 3 do niniejszej Instrukcji.

11. Postanowienia końcowe

1. Użytkownikom, korzystającym z systemu informatycznego, zabrania się instalowania na komputerach jakiegokolwiek oprogramowania, jeżeli nie są do tego uprawnieni.
2. 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.
3. ABI prowadzi okresową kontrolę przestrzegania zasad ochrony danych osobowych w Urzędzie Gminy we Frysztaku.
4. Dane osobowe, przekazane do przetwarzania innemu podmiotowi, na podstawie umowy, mogą być przetwarzane tylko w zakresie i celu określonym w umowie.
5. Odpowiedzialność za przestrzeganie procedur, dotyczących bezpieczeństwa danych powierzonych innemu podmiotowi, o których mowa w ust. 1, spoczywa na Administratorze Danych Osobowych oraz podmiocie, z którym zawarto umowę.
6. Pracownicy Urzędu Gminy we Frysztaku są odpowiedzialni za przestrzeganie procedur przetwarzania danych osobowych, określonych przez Administratora Danych Osobowych.
7. 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.
8. Administrator Systemu Informatycznego lub inne osoby upoważnione, zobowiązani są do uwzględniania warunków bezpieczeństwa danych osobowych przy wprowadzeniu rozwiązań programowych i sprzętowych, służących do przetwarzania danych.
9. W sprawach nieuregulowanych niniejszą Instrukcją mają zastosowanie przepisy ustawy o ochronie danych osobowych oraz odrębne akty, regulaminy dotyczące bezpieczeństwa teleinformatycznego.

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:.....	
1. Nazwa systemu:..... 2. Rodzaj uprawnień: ..... ….. /podgląd, modyfikacja, administrowanie/*	
A. Uzasadnienie wniosku:	
....	
..... /data/ ..... /podpis i pieczątka/	
Potwierdzam nadanie/odebranie* uprawnień dla użytkownika o identyfikatorze: .... /data/ ..... /podpis i pieczątkaASI/	
Potwierdzam wpisanie danych do ewidencji. ..... /data/ ..... /podpis i pieczątka ABI/	

* *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):

	Osoby uczestniczące w zdarzeniu (Nazwisko, imię, podpis, data)	*Administrator Bezpieczeństwa Informacji (Nazwisko, imię, podpis, data)*	*Administrator Systemu Informatycznego (Nazwisko, imię, podpis, data)*
1)			
2)			
3)			

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 jakiekolwiek 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 jakiekolwiek 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.				

Administrator Systemu Informatycznego

_____
Data i podpis

Administrator Bezpieczeństwa Informacji

_____
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

L.p.	Nr umowy	Jednostka organizacyjna	Podmiot			Pracownicy podmiotu		
			Nazwa	Miasto, Adres	NIP	Imię	Nazwisko	Nr upoważnienia wydanego przez Administratora