Załącznik nr 2 do Zarządzenia nr 78/2016.
Wójta Gminy Szreńsk
z dnia 21.04.2016 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

Dotyczy przetwarzania danych osobowych za pośrednictwem systemów informatycznych w Gminie Szreńsk.

Dokumentację opracowano zgodnie z:

- Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jednolity: Dz. U. 2015 r. poz. 2135 z późn. zm.*),
- Ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (*tekst jednolity: Dz. U. 2014 r. poz. 1114 z późn. zm.),*
- Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (*Dz. U. 2012 r. poz. 526),*
- Rozporządzeniem 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 2004 r. nr 100, poz. 1024*).

Zatwierdził
WÓJT
Marek Nitczyński
Podpis Administratora
Danych Osobowych

Spis treści:

Postanowienia Ogólne

§ 1

1. Niniejsza instrukcja dotyczy wszystkich zbiorów danych osobowych przetwarzanych w Gminie Szreńsk za pośrednictwem systemów informatycznych.

2. Administrator Danych Osobowych stale nadzoruje procedury określone w dokumentacji Instrukcji Zarządzania Systemami Informatycznymi pod kątem aktualności, poprawności, spójności i zgodności z przepisami prawa.

3. Każda osoba przetwarzająca dane osobowe za pośrednictwem systemów informatycznych zobowiązana jest do zapoznania się z treścią Instrukcji Zarządzania Systemami Informatycznymi oraz do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień w nich zawartych.

4. Osoba przetwarzająca dane osobowe w systemie informatycznym zobowiązana jest złożyć oświadczenie o tym, że została zaznajomiona z obowiązującą Instrukcją Zarządzania Systemami Informatycznymi. Administrator Systemów Informatycznych ewidencjonuje oświadczenia osób zaznajomionych z zasadami określonymi w Instrukcji Zarządzania Systemem Informatycznym *(wzór ewidencji określa **załącznik nr 3** dokumentacji Instrukcji Zarządzania Systemami Informatycznymi)*.

5. Dostęp do pomieszczeń, w którym przetwarzane są dane osobowe w systemach informatycznych jest zabezpieczony przed dostępem osób nieuprawnionych na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych poprzez wprowadzenie środków technicznych i organizacyjnych określonych w Polityce Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych.

6. Dostęp do pomieszczenia/ń, w którym znajduje/ą się serwer/y posiadają wyłącznie osoby upoważnione przez Administratora Danych Osobowych.

7. Dokładną lokalizację elementów wchodzących w skład infrastruktury informatycznej określa **załącznik nr 2** dokumentacji Instrukcji Zarządzania Systemami Informatycznymi.

Użyte w Instrukcji określenia

§ 2

1. **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

2. **Administrator Danych Osobowych (ADO)** – Gmina Szreńsk reprezentowany przez Wójta Gminy Szreńsk.

3. **Administrator Bezpieczeństwa Informacji (ABI)** - osoba powołana przez Administratora Danych Osobowych na podstawie art 36, ust. 1 Ustawy o Ochronie Danych Osobowych (*tekst jednolity: Dz.U. 2015 r. poz. 2135 z późn. zm.*). odpowiedzialna za bezpieczeństwo danych osobowych, przetwarzanych zarówno w formie tradycyjnej jak i za pomocą systemów informatycznych;

4. **Administrator Systemów Informatycznych (ASI)** – osoba powołana przez Administratora Danych Osobowych odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych za pomocą systemów informatycznych;

5. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

6. **Stacja robocza** – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

7. **Przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.

8. **Osoba upoważniona** - osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych lub osobę przez niego uprawnioną dopuszczona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu (*wzór upoważnienia stanowi* ***załącznik nr 5*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych)* oraz wykazana w ewidencji upoważnień *(wzór*

*ewidencji stanowi **załącznik nr 6** dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych).*

9. **Użytkownik systemu** - osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym.

10. **Ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych *(tekst jednolity: Dz. U. 2015 r. poz. 2135 z późn. zm.)*.

11. **Rozporządzenie** - rozporządzenie 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. 2004 r. nr 100, poz. 1024).*

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

§ 3

1. Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych (*wzór upoważnienia stanowi **załącznik nr 5** dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych).*

2. Administrator Systemów Informatycznych jest zobowiązany do prowadzenia ewidencji pracowników upoważnionych do przetwarzania danych osobowych *(wzór ewidencji stanowi **załącznik nr 6** dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych)*. Zgodnie z art. 39 ust. 1 Ustawy taka ewidencja zawiera:

   1) imię i nazwisko osoby upoważnionej;
   2) przypisany tej osobie identyfikator;
   3) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych.

3. Identyfikator i hasło do systemu informatycznego przetwarzającego dane osobowe są przydzielane użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych wydane przez Administratora Danych Osobowych lub osobę przez niego uprawnioną.

4. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie

korzystał z systemu informatycznego odpowiada Administrator Systemów Informatycznych.

6. Oryginał upoważnienia zostaje przekazany pracownikowi za potwierdzeniem odbioru, kopia zostaje dołączona do akt osobowych pracownika oraz przekazana do wiadomości przełożonego pracownika.

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 4

1. System informatyczny służący do przetwarzania danych osobowych posiada mechanizm uwierzytelniający użytkownika, mechanizmy pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).

2. Dostęp do systemu informatycznego, w którym użytkownik systemu będzie przetwarzał dane osobowe może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.

3. Identyfikator wpisuje się do ewidencji upoważnień prowadzonej przez Administratora Systemów Informatycznych *(wzór ewidencji stanowi* ***załącznik nr*** *6 dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych).*

4. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie. System informatyczny przetwarzający dane osobowe jest skonfigurowany w sposób wymagający bezpieczne zarządzanie hasłami użytkowników.

5. Hasła są poufne i muszą być zmieniane nie rzadziej niż raz na 30 dni przez użytkownika. Ponadto hasło musi składać się przynajmniej z ośmiu znaków, zawierać przynajmniej jedną wielką i małą literę oraz cyfry lub znaki specjalne.

6. W przypadku braku możliwości uzyskania dostępu do systemu informatycznego, użytkownik systemu zobowiązany jest powiadomić Administratora Systemów Informatycznych, który w

zależności od mechanizmu działania systemu korzysta z opcji przypomnienia hasła, bądź nadania nowego.

7. W sytuacji podejrzenia naruszenia bezpieczeństwa działania systemu informatycznego służącego do przetwarzania danych osobowych (brak możliwości zalogowania pomimo wprowadzenia poprawnego identyfikatora oraz hasła lub stwierdzenie fizycznej ingerencji) użytkownik zobowiązany jest powiadomić Administratora Systemów Informatycznych, który przeprowadza sprawdzenie doraźne zgodnie z procedurą określoną w Polityce Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych.

8. Nie rzadziej niż raz do roku przeprowadzana jest kontrola uprawnień użytkowników pod kątem posiadania przez użytkowników stosownych uprawnień do realizowanych zadań oraz obowiązków.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

§ 5

1. Przed rozpoczęciem pracy w systemie informatycznym służącym do przetwarzania danych osobowych oraz w jej trakcie każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych.

2. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

3. W przypadku bezczynności użytkownika przez okres dłuższy niż 10 minut automatycznie włączany jest wygaszacz ekranu. Wznowienie pracy możliwe jest wyłącznie po ponownym podaniu danych użytkownika.

4. Zmianę użytkownika systemu informatycznego każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jeden identyfikator. W przypadku, gdy przerwa w pracy ma trwać dłużej niż 60 minut użytkownik obowiązany jest wylogować się z systemu informatycznego oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji zawierające dane osobowe. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne monitory stanowisk dostępu do danych są ustawione w taki sposób żeby uniemożliwić tym

osobom wgląd w dane.

5. Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z systemu.

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

§ 6

1. W związku z tym, że systemy informatyczne narażone są na działanie szkodliwego oprogramowania, którego celem jest zniszczenie, zmienienie lub umożliwienie osobom nieupoważnionym do danych osobowych konieczne jest podjęcie odpowiednich środków ochronnych.

2. Można wyróżnić następujące rodzaje występujących tu zagrożeń:

   1) nieuprawniony dostęp bezpośrednio do danych osobowych;
   2) uszkodzenie kodu aplikacji umożliwiającej dostęp danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu;
   3) przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci publicznej;
   4) przechwycenie danych z aplikacji umożliwiającej dostęp do bazy danych systemu informatycznego wykorzystywanego do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych;
   5) uszkodzenie lub zafałszowanie danych osobowych przez szkodliwe oprogramowanie zakłócające pracę aplikacji umożliwiającej dostęp do bazy danych systemu informatycznego wykorzystywanego do przetwarzania danych osobowych.

3. Potencjalnymi źródłami przedostawania się szkodliwego oprogramowania na stacje robocze są :

   1) załączniki do poczty elektronicznej;
   2) przeglądane strony internetowe;
   3) pliki i aplikacje pochodzące z sieci publicznej lub z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

4. W celu zminimalizowania zagrożeń zabrania się wykorzystywania prywatnego sprzętu przez pracowników do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych.

5. W celu zapewnienia ochrony przed szkodliwym oprogramowaniem Administrator Systemów Informatycznych jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym szkodliwe oprogramowanie. System ten jest skonfigurowany w następujący sposób:

   1) rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) jest stale włączony;
   2) skaner ruchu internetowego (zapora ogniowa) jest stale włączony;
   3) monitor zapewniający ochronę przed wirusami makr w arkuszach kalkulacyjnych oraz edytorach tekstu jest stale włączony;
   4) skaner poczty elektronicznej jest stale włączony.

6. System skonfigurowany jest w taki sposób, iż nie rzadziej niż raz dziennie automatycznie dokonuje sprawdzenia możliwości aktualizacji bazy wirusów oraz szkodliwego oprogramowania i automatycznie jej dokonuje.

7. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy użytkownik zobowiązany jest powiadomić Administratora Danych Osobowych, który podejmuje działania zmierzające do usunięcia zagrożenia.

8. W szczególności działania te mogą obejmować :

   1) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego;
   2) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub po skonsultowaniu się z zewnętrznymi ekspertami.

§ 7

1. Systemy informatyczne odnotowują:

   1) datę pierwszego wpisu do systemu;
   2) identyfikator użytkownika wprowadzającego dane osobowe do systemu;
   3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
   4) informacje o odbiorach danych osobowych;
   5) informacji o wniesieniu sprzeciwu wobec przetwarzania danych osobowych.

2. Odnotowanie to odbywa się automatycznie.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, systemy zapewniają sporządzenie i wydrukowanie raportu zawierającego następujące informacje:

   1) datę pierwszego wpisu do systemu;
   2) identyfikator użytkownika wprowadzającego dane osobowe do systemu;
   3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,
   4) informacji o wniesieniu sprzeciwu wobec przetwarzania danych osobowych.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

§ 8

1. Częstotliwość prac związanych z naprawą i konserwacją elementów wchodzących w skład infrastruktury informatycznej zależna jest od specyfiki tego elementu, zainstalowanego na nim systemu operacyjnego, oprogramowania, ilości użytkowników z niego korzystających oraz częstotliwości wykorzystywania.

2. Wszelkie prace związane z naprawami i konserwacją elementów wchodzących w skład infrastruktury informatycznej muszą uwzględniać zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych. Prace serwisowe prowadzone w tym zakresie mogą być wykonywane wyłącznie przez upoważnione do tego przez Administratora Danych Osobowych osoby.

3. Przed rozpoczęciem prac serwisowych przez osoby postronne konieczne jest potwierdzenie tożsamości serwisantów. Urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe, przeznaczone do:

   1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
   3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej.

4. Dane z nośników usuwa się poprzez:

   1) nadpisanie danych poprzez wykorzystanie specjalistycznego oprogramowania,
   2) demagnetyzacja - w przypadku magnetycznych nośników danych,

5. Administrator Danych Osobowych w momencie zawierania umowy na zakup urządzeń zawierających nośniki danych osobowych (np. komputery stacjonarne, notebooki, netbooki, tablety, telefony, urządzenia wielofunkcyjne) zobowiązany jest podjąć negocjacje mające na celu umożliwienie oddania do naprawy urządzenia pozbawionego dysku twardego. Ewentualna odmowa zawarcia takiego zapisu przez gwaranta wymaga formy pisemnej.

Tworzenie oraz przechowywanie kopii zapasowych

§ 9

1. Dane osobowe przetwarzane w systemach informatycznych zabezpieczone są przed utratą lub zmienieniem poprzez wykonywanie okresowych kopii zapasowych.

2. Nośniki elektroniczne zawierające kopie zapasową zbiorów danych osobowych przechowywane są w innych pomieszczeniach niż systemy informatyczne, na których zostały utworzone w sposób uniemożliwiający dostęp do nich przez osoby nieupoważnione.

3. Wszystkie kopie zapasowe zbiorów danych osobowych przetwarzanych za pośrednictwem systemów

informatycznych wykonuje się metodą kopii pełnej.

4. Systemy informatyczne są skonfigurowane w taki sposób, że kopie danych osobowych wykonywane są automatycznie.

5. Częstotliwość dokonywania kopii zapasowej poszczególnych zbiorów, rodzaj nośnika, na którym przechowywane są dane osobowe oraz miejsce przechowywania nośnika, określa **załącznik nr 1** dokumentacji Instrukcji Zarządzania Systemami Informatycznymi.

6. Okres przechowywania kopii zapasowej zależny jest od częstotliwości jej wykonywania:

   1) kopia zapasowa wykonywana codziennie – przechowywana przez okres jednego tygodnia;
   2) kopia zapasowa wykonywana raz w tygodniu – przechowywana przez okres jednego miesiąca;
   3) kopia zapasowa wykonywana raz w miesiącu – przechowywana przez okres jednego roku;
   4) kopia zapasowa wykonywana raz w roku – przechowywana przez okres 5 lat.

Sposób spełnienia wymogów względem systemów informatycznych

§ 10

1. Systemy informatyczne wykorzystywane do przetwarzania danych osobowych wyposażone są w mechanizmy automatycznego tworzenia systemowych dzienników zdarzeń.

2. Dzienniki te odnotowują działania użytkowników lub obiektów systemowych polegające na dostępie do:

   a. Systemu z uprawnieniami administracyjnymi,
   b. Konfiguracji systemu, w tym konfiguracji zabezpieczeń,

3. Dzienniki te odnotowują również informacje o:

   a. Działaniach użytkowników nieposiadających uprawnień administracyjnych,
   b. Zdarzeniach systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu,

4. Opis przepływ informacji pomiędzy systemami informatycznymi, a siecią publiczną został zapewniony poprzez system automatycznego tworzenia dziennika zdarzeń tworzonych przez urządzenia infrastruktury sieciowej.

5. Każdy fakt podłączania sprzętu zewnętrznego do infrastruktury sieciowej jest zapisany w dzienniku zdarzeń automatycznie tworzonym przez elementy wchodzące w skład infrastruktury sieciowej.

6. Systemy informatyczne zostały wyposażone w system podtrzymywania napięcia w postaci:
    a. Komputery przenośne – baterie,
    b. Komputery stacjonarne – zasilacze awaryjne,

7. Komputery przenośne oraz dyski zewnętrzne należące do Gminy Szreńsk, które są wykorzystywane do przetwarzania danych osobowych poza obszarem przetwarzania, zabezpieczone są przed dostępem osób nieupoważnionych za pomocą oprogramowania szyfrującego dane.

8. Systemy informatyczne wykorzystywane do przesyłania danych w sieci publicznej zapewniają kryptograficzne zabezpieczenie przesyłanych danych.

9. Nie rzadziej niż raz do roku przeprowadzana jest inwentaryzacja sprzętu oraz oprogramowania służącego do przetwarzania danych osobowych.

10. Nie rzadziej niż raz do roku przeprowadzana jest kontrola uprawnień użytkowników pod kątem posiadania przez użytkowników stosownych uprawnień do realizowanych zadań oraz obowiązków.

11. Nie rzadziej niż raz na pół roku przeprowadzana jest analiza dostępności aktualizacji firmware (oprogramowania sprzętowego) elementów wchodzących w skład infrastruktury sieciowej. Na podstawie przeprowadzanej analizy, instalowana jest najnowsza dostępna wersja oprogramowania.

Załącznik nr 1
do Instrukcji Zarządzania Systemami Informatycznymi
w Gminie Szreńsk

ZESTAWIENIE INFORMACJI DOTYCZĄCYCH WYKONYWANIA ORAZ PRZECHOWYWANIA KOPII ZAPASOWYCH

Lp.:	Nazwa zbioru:	Częstotliwość wykonywania kopii zapasowej	Rodzaj nośnika:	Sposób wykonania kopii zapasowej:	Miejsce przechowywania:
1	Ewidencja ludności Gminy Szreńsk	codziennie	Dysk lokalny	Przez pracownika	Pokój nr 7
2	Ewidencja podatników, płatników i dłużników	codziennie	Dysk zewnętrzny	automatycznie	
3	Zwrot podatku akcyzowego	codziennie	Dysk zewnętrzny	automatycznie	
4	Płace	codziennie	Dysk zewnętrzny	automatycznie	
5	Księgowość budżetowa	codziennie	Dysk zewnętrzny	automatycznie	
6	Ubezpieczenie pracowników w ZUS	Raz na miesiąc	Dysk zewnętrzny	Przez pracownika	
7	Rejestr wyborców	codziennie	Dysk lokalny	Przez pracownika	
8	Inwentaryzacja wyrobów zawierających azbest	Raz na miesiąc	Na serwerze Small GIS Kraków	automatycznie	

9	Zbiór wniosków o wpis do Centralnej Ewidencji i Informacji o Działalności Gospodarczej	Raz na miesiąc			

Załącznik nr 2
do Instrukcji Zarządzania Systemami Informatycznymi
w Gminie Szreńsk

LOKALIZACJA ELEMENTÓW WCHODZĄCYCH W SKŁAD INFRASTRUKTURY INFORMATYCZNEJ

I. Elementy infrastruktury sieciowej (modemy, routery, switch'e, hub'y):

Lp.:	Nazwa i model urządzenia	Lokalizacja
1	Modem Router DSL „ Comtrend"	sekretariat
2	Router D- Link	sekretariat
3	Switch Cisco	sekretariat
4	Switch D- Link	serwerowani
5		

II. Elementy służące do przetwarzania danych osobowych (serwery, stacje robocze, terminale, dyski sieciowe):

Lp.:	Nazwa / model	Lokalizacja	Zastosowana metoda dostępu
1	Serwer PC	Serwerownia	Dostęp bezpośredni / za pośrednictwem sieci lokalnej
2	Serwer z projektu EA	Serwerownia	Sieć lokalna
3			
4			
5			
6			
7			

Załącznik nr 3
do Instrukcji Zarządzania Systemami Informatycznymi
w Gminie Szreńsk

EWIDENCJA OSÓB

zapoznanych z „Instrukcją Zarządzania Systemami Informatycznymi" w Gminie Szreńsk

PRZYJĄŁEM/AM DO WIADOMOŚCI I STOSOWANIA ZAPISY INSTRUKCJI ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

Lp.	Nazwisko i imię	Data i podpis