Załącznik Nr 2
do Zarządzenia Nr 73/16
Wójta Gminy Srokowo
z dnia 23 sierpnia 2016 r.

Instrukcja Zarządzania Systemami Informatycznymi w Urzędzie Gminy Srokowo

Sporządził: Data:	Sprawdził: Data:	Zatwierdził: Data:

Spis treści

1. Postanowienia Ogólne

1.1. Podstawa prawna

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922) oraz 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. z 2004 r., Nr 100, poz. 1024 ze zm.)

1.2. Zakres stosowania

Instrukcja Zarządzania Systemami Informatycznymi w Urzędzie Gminy Srokowo, zwana dalej Instrukcją, opisuje sposoby nadawania uprawnień użytkownikom, określa sposób pracy w systemie informatycznym, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego Urzędu Gminy Srokowo. Instrukcja obowiązuje wszystkie komórki organizacyjne Urzędu oraz wszystkich pracowników.

1.3. Definicje

Urząd – Urząd Gminy Srokowo

Ustawa – Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. z 2016 r., poz. 922)

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. z 2004 r., Nr 100, poz. 1024 ze zm.)

ADO – Administrator Danych Osobowych

ASI – Administrator Systemów Informatycznych

ABI – Administrator Bezpieczeństwa Informacji - rozumie się przez to osobę, której Administrator Danych Osobowych powierzył nadzór nad zapewnieniem przestrzegania przepisów o ochronie danych osobowych, nadzorowanie opracowania i aktualizowania dokumentacji oraz prowadzenie rejestru zbiorów danych

PBI – Polityka Bezpieczeństwa Informacji – dokument realizujący wymóg art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

Użytkownik systemu – osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym Urzędu, pracownik Urzędu lub pracownik innego podmiotu, który świadczy usługi związane z działalnością statutową Urzędu

Sieć lokalna (LAN) – połączenie systemów informatycznych Urzędu wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych

2. Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym

2.1. Zasady nadawania uprawnień

Przetwarzać dane, w tym dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych. Nadanie przez Administratora Danych Osobowych upoważnienia oraz rejestracja użytkownika systemu informatycznego przetwarzającego dane osobowe następuje na wniosek przełożonego użytkownika. Składa on wniosek do Administratora Bezpieczeństwa Informacji o wydanie upoważnienia do przetwarzania danych osobowych.

Wniosek o upoważnienie osoby niebędącej pracownikiem składa osoba upoważniona lub Administrator Systemu Informatycznego.

Wniosek ten powinien zawierać:

1) Imię i nazwisko osoby, której upoważnienie zostanie nadane
2) Zakres upoważnienia do przetwarzania danych osobowych
3) Datę, z jaką upoważnienie ma być nadane

Oryginał upoważnienia zostaje przekazany osobie upoważnionej za potwierdzeniem odbioru, kopia zostaje dołączona do akt PBI.

O okresie upoważnienia decyduje Administrator Danych Osobowych.

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.

Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada właściwy Administrator Systemu Informatycznego. Identyfikator użytkownika zostaje wpisany do Rejestru osób upoważnionych oraz do upoważnienia do przetwarzania danych osobowych.

Wyrejestrowanie użytkownika z systemu informatycznego może nastąpić na wniosek Administratora Danych Osobowych, Administratora Bezpieczeństwa Informacji lub przełożonego użytkownika. Zgłoszenie ustania potrzeby powierzenia danych osobowych zgłasza się na wniosku.

Pisemny wniosek o wyrejestrowanie użytkownika systemu należy złożyć do Administratora Bezpieczeństwa Informacji. Wyrejestrowanie użytkownika oraz cofnięcie upoważnienia do przetwarzania danych osobowych następuje również w sytuacji rozwiązania stosunku pracy pomiędzy Urzędem a pracownikiem. Wyrejestrowanie użytkownika z systemu realizuje Administrator

Systemów Informatycznych na podstawie pisemnego wniosku lub karty obiegowej pracownika. Jednocześnie bezpośredni przełożony użytkownika rozlicza go z przekazanych mu aktywów (o ile były mu wydane).

Administrator Bezpieczeństwa Informacji jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych, w tym danych osobowych.

Zgodnie z art. 39 ust. 1 ustawy taka ewidencja zawiera:

1) Imię i nazwisko osoby upoważnionej
2) Datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych
3) Identyfikatory nadane w systemach

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

3.1. Identyfikator i hasło

Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonywane przy użyciu identyfikatora, którym się posługuje lub posługiwał.

Identyfikator składa się minimalnie z ośmiu znaków, znaki identyfikatora nie są rozdzielane spacjami ani znakami interpunkcyjnymi.

Identyfikator wpisuje się do ewidencji, prowadzonej przez Administratora Bezpieczeństwa Informacji, wraz z imieniem i nazwiskiem użytkownika oraz nazwami systemów informatycznych, do których użytkownik uzyskał dostęp i wprowadzany jest przez Administratora Systemów Informatycznych do właściwych systemów.

Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.

3.2. System informatyczny przetwarzający dane osobowe

System informatyczny przetwarzający dane osobowe jest konfigurowany w sposób wymagający bezpieczne zarządzanie hasłami użytkowników:

a) Hasło przydzielone użytkownikowi musi być zmienione po pierwszym udanym zalogowaniu się do systemu informatycznego przetwarzającego dane osobowe
b) Hasła są zmieniane przez użytkownika
c) System informatyczny wyposażony jest w mechanizmy wymuszające zmianę hasła po upływie 30 dni od dnia ostatniej zmiany hasła

d) System informatyczny wyposażony jest w mechanizm pozwalający na wymuszenie jakości hasła
e) Hasło powinno składać się z co najmniej 8 znaków. Hasło powinno zwierać małe i wielkie litery oraz cyfry lub znaki specjalne

4. Procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla użytkowników systemu

a) Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każda osoba obowiązana jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych. Szczegółowy opis takich symptomów oraz sposób postępowania w przypadku ich wykrycia został opisany w dokumencie „Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych w Urzędzie Gminy Srokowo".
b) 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.
c) Po przekroczeniu określonej dla wybranego systemu liczby prób logowania, system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowanie konta dokonuje Administrator Systemów Informatycznych.
d) W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 15 minut automatycznie włączany jest wygaszacz ekranu. Wznowienie pracy po wygaszeniu ekranu wymagać musi ponownego podania hasła użytkownika.
e) Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika.
f) Zakończenie pracy w systemie informatycznym dokonuje się poprzez wylogowanie użytkownika ze wszystkich aplikacji oraz systemu operacyjnego komputera.
g) W pomieszczeniach w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
h) W przypadku, gdy pracownik opuszcza czasowo stanowisko pracy, obowiązany jest zablokować stację roboczą lub wylogować się z aplikacji i systemu stacji roboczej, na której pracuje oraz sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji zawierające dane osobowe. Wznowienie pracy w systemach operacyjnych oraz systemach przetwarzających dane, w tym dane osobowe może nastąpić jedynie po podaniu hasła użytkownika.

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

a) Dane, w tym dane osobowe przetwarzane w systemach informatycznych Urzędu, podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada Administrator Systemu Informatycznego lub osoba specjalnie do tego celu wyznaczona.
   W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych użytkownicy systemu informatycznego zobowiązani są do zapisywania danych w wyznaczonych do tego celu folderach, tak aby możliwe było zabezpieczenie ich dostępności poprzez wykonanie kopii zapasowych. Każda stacja robocza ma wyznaczony folder systemowy, np. pulpit, moje dokumenty, którego zawartość jest automatycznie zapisywana na serwerze raz dziennie.
b) Kopie zapasowe informacji przechowywanych w systemie informatycznym przetwarzającym dane osobowe tworzone są w następujący sposób:
   - System PUMA – pełna kopia bazy jest wykonywana codziennie i przechowywana na dwóch serwerach Urzędu Gminy Srokowo w postaci zabezpieczonego szyfrowanym hasłem archiwum oraz wysyłana połączeniem szyfrowanym na jeden serwer Urzędu Marszałkowskiego
   - System Płatnik – pełna kopia bazy jest wykonywana codziennie i przechowywana na dwóch serwerach Urzędu Gminy Srokowo w postaci zabezpieczonego szyfrowanym hasłem archiwum
   - System EWOPIS 6 – pełna kopia bazy jest wykonywana codziennie i przechowywana na dwóch serwerach Urzędu Gminy Srokowo w postaci zabezpieczonego szyfrowanym hasłem archiwum
   - Raz na dwa tygodnie jest wykonywana kopia całych systemów operacyjnych serwera i przechowywana na dwóch serwerach
c) Kopie zapasowe bazy danych osobowych mające wpływ na ciągłość działań Urzędu są testowane nie rzadziej jak raz na kwartał.
d) Nośniki kopii zapasowych, które zostały wycofane z użycia pozbawiane są zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych dla typu nośnika, w sposób uniemożliwiający odczytanie zapisanych na nich danych, protokolarnie potwierdzonym przez Administratora Bezpieczeństwa Informacji lub specjalistyczną firmę dokonującą kasowania danych.
e) Ponadto:
   - Zbiory danych przechowywane są na serwerze obsługującym system informatyczny Urzędu. Wszelkie dane przetwarzane w pamięci poszczególnych stacji roboczych oraz komputerów przenośnych są niezwłocznie umieszczane w odpowiednich, przydzielonych dla danego użytkownika przez Administratora Systemów Informatycznych miejscach na serwerze lub innych wskazanych i określonych lokalizacjach.
   - Zakazuje się zapisywania danych chronionych, w tym danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych bez zaszyfrowania.

Przesyłanie korespondencji wewnątrz Urzędu może odbywać się bez zabezpieczeń. Przesyłanie danych chronionych na zewnątrz może odbywać się jedynie po zabezpieczeniu informacji poprzez hasło dostępu, spełniające wymogi opisane w pkt. 3.2.e.

- W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego, użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym.
- Nośniki magnetyczne raz użyte do przetwarzania danych osobowych mogą być wykorzystywane do innych celów, tylko po nadpisaniu danych w trybie kasowania formatującego przy zastosowaniu specjalistycznego oprogramowania lub demagnetyzacji. Nośniki na których nie można powtórnie zapisać informacji powinny być niszczone poprzez pocięcie, zgniecenie, demagnetyzację lub spopielenie.
- Przenośne nośniki danych z zaszyfrowanymi, jednostkowymi danymi osobowymi są – na czas ich użyteczności, przechowywane w zamkniętych na klucz szafach, a po wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki są niszczone poprzez pocięcie, zgniecenie, demagnetyzację lub spopielenie.
- Po wygaśnięciu okresu przydatności tychże kopii (zastąpieniu ich przez aktualne wersje lub zakończeniu okresu trwałości), są one trwale kasowane lub nośniki je przechowujące niszczone są mechanicznie.

6. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

a) Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej lub z wykorzystaniem do tego celu sieci informatycznej stosując bezpieczne szyfrowane połączenie.
b) Nośniki elektroniczne, zawierające bazy danych, w tym danych osobowych powinny być przechowywane wewnątrz obszaru przeznaczonego do przetwarzania danych osobowych i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników danych, o których mowa powyżej, poza gmach Urzędu powinno odbywać się za wiedzą Administratora Bezpieczeństwa Informacje.
c) W przypadku, gdy nośnik danych, w tym danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika. Jeżeli wydruk danych, w tym danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki, zapewniającej odpowiednie zniszczenie dokumentu.
d) W przypadku, gdy kopia zapasowa nie jest dłużej potrzebna, należy przeprowadzić jej zniszczenie lub usunięcie danych z nośnika, na którym się ona znajduje.
e) W przypadku dokonania brakowania dokumentów tradycyjnych lub przekazania ich do Archiwum Państwowego, należy odpowiadające im zapisy w bazach danych usunąć lub

zabezpieczyć przed ich odczytaniem. Dokonanie brakowania dokumentów tradycyjnych, potwierdzone protokołem brakowania musi być skorelowane z protokołem brakowania (usunięcia) zapisów z baz danych na serwerach, stacjach roboczych a także z bieżących i archiwalnych kopii bezpieczeństwa.

f) Jeżeli brakowanie danych, znajdujących się w kopiach baz danych jest niemożliwe lub nieuzasadnione ze względów ekonomicznych, kopia, w której znajdują się dane objęte brakowaniem musi zostać odpowiednio oznaczona. Nadzór nad tym, żeby część danych objętych brakowaniem nie została ponownie użyta spoczywa na Administratorze Bezpieczeństwa Informacji.

7. Zabezpieczenie przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

a) W związku z tym, że system informatyczny narażony jest na działanie oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu konieczne jest podjęcie odpowiednich środków ochronnych.
Można wymienić następujące rodzaje występujących tu zagrożeń:
   - Nieuprawniony dostęp bezpośrednio do bazy danych
   - Uszkodzenie kodu aplikacji umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu
   - Przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci Internet
   - Przechwycenie danych z aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych
   - Uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy zakłócający pracę aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych

b) W celu przeciwdziałania wymienionym zagrożeniom system informatyczny musi posiadać następujące zabezpieczenia:
   - Logiczne odseparowanie serwera bazy danych od sieci zewnętrznej
   - Autoryzacja użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu
   - Stosowanie rygorystycznego systemu autoryzacji dostępu do wszystkich serwerów, na których znajdują się elementy aplikacji umożliwiających przetwarzanie danych osobowych
   - Stosowanie aplikacji w postaci skompilowanej i nie umieszczenie kodu źródłowego aplikacji na powszechnie dostępnych serwerach
   - Stosowanie szyfrowanej transmisji danych przy zastosowaniu odpowiedniej długości klucza szyfrującego

- Stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych

c) Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:
   - Załączniki poczty elektronicznej
   - Przeglądane strony internetowe
   - Pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej

d) W celu zapewnienia ochrony antywirusowej Administrator Systemu Informatycznego przetwarzającego dane osobowe lub osoba specjalnie do tego wyznaczona, jest odpowiedzialna za zarządzanie systemem wykrywającym i usuwającym wirusy. System antywirusowy powinien być skonfigurowany w następujący sposób:
   - Rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony
   - Antywirusowy skaner ruchu internetowego powinien być stale włączony
   - Skaner poczty elektronicznej powinien być stale włączony

e) Systemy antywirusowe zainstalowane na stacjach roboczych powinny być skonfigurowane w następujący sposób:
   - Zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego, o ile pozwalają na to możliwości techniczne
   - Skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów – na bieżąco
   - Skanowania zawartości dysków stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – na bieżąco

   System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.

f) Użytkownicy systemu informatycznego zobowiązani są do:
   - Skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – przy każdym odczycie
   - Nie ingerowania w ustawienia konfiguracyjne systemu antywirusowego
   - Natychmiastowego powiadomienia ASI o zauważonych przypadkach wykrycia zagrożeń przez oprogramowanie antywirusowe

g) W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy Administrator Systemu Informatycznego lub inny wyznaczony pracownik powinien podjąć działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
   - Usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego
   - Odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane

- Samodzielną ingerencję w zawartość pliki – w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami

h) System informatyczny przetwarzający dane osobowe powinien posiadać mechanizmy pozwalające na zabezpieczenie przed ich utratą lub wystąpieniem zafałszowania w wyniku awarii zasilania lub zakłóceń w sieci zasilającej. W związku z tym system informatyczny powinien być wyposażony w co najmniej:
   - Filtry zabezpieczające stacje robocze przed skutkami przepięcia
   - Zasilacze awaryjne serwerów baz danych, serwerów aplikacji oraz urządzeń pamięci masowej pozwalające na bezpieczne zamknięcie aplikacji przetwarzających dane osobowe w sposób umożliwiający poprawne zapisanie przetwarzanych danych

8. Realizacja wymogu uwierzytelnienia użytkownika i rejestracji zdarzeń

System informatyczny przetwarzający dane, w tym dane osobowe musi posiadać mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Powinien także posiadać mechanizmy pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).

a) System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:
   - Rozpoczęcie i zakończenie pracy przez użytkownika systemu
   - Operacje wykonywane na przetwarzanych danych, a w szczególności ich dodanie, modyfikację oraz usunięcie
   - Przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będący właścicielem ani współwłaścicielem system
   - Nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych
   - Błędy w działaniu systemu informatycznego podczas pracy danego użytkownika. Zapis działań użytkownika uwzględnia:
     - Identyfikator użytkownika
     - Datę i czas w którym zdarzenie miało miejsce
     - Rodzaj zdarzenia
     - Określenie informacji, których zdarzenie dotyczy (identyfikatory rekordów)

b) W ramach możliwości technicznych system informatyczny powinien posiadać mechanizmy pozwalające na automatyczne powiadomienie Administratora Bezpieczeństwa Informacji lub osobę przez niego uprawnioną o zaistnieniu zdarzenia krytycznego (mogącego mieć krytyczne znaczenie dla bezpieczeństwa przetwarzanych danych osobowych)

c) Administrator Systemów Informatycznych dokonuje regularnego przeglądu uprawnień poprzez przegląd kont użytkowników w tym kontroli stanowisk z udzielonymi przywilejami

d) Administrator Danych Osobowych lub Administrator Bezpieczeństwa Informacji dokonuje okresowego praw użytkowników w sytuacji zmiany zakresu obowiązków pracowników lub Regulaminu Organizacyjnego
e) Ponadto system informatyczny powinien zapewnić zapis faktu przekazania danych, w tym danych osobowych z uwzględnieniem:
    - Identyfikatora osoby, której dane dotyczą
    - Osoby przesyłającej dane
    - Odbiorcy danych
    - Zakresu przekazanych danych osobowych
    - Daty operacji
    - Sposobu przekazania danych

9. Przegląd i konserwacja systemów oraz nośników informacji służących do przetwarzania danych

a) Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych
b) Prace serwisowe na terenie Urzędu prowadzone w tym zakresie mogą być wykonywane wyłącznie przez pracowników Urzędu lub przez upoważnionych przedstawicieli wykonawców zewnętrznych będących pod nadzorem pracowników Urzędu
c) Przed rozpoczęciem prac serwisowych przez osoby spoza Urzędu, a nie będących pracownikami Urzędu, konieczne jest potwierdzenie tożsamości serwisantów
d) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane, w tym dane osobowe, przeznaczone do:
    - Likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie
    - Przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie
    - Naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych, chyba, że świadczący usługi serwisowe został upoważniony do przetwarzania danych chronionych
e) Wszelkie prace serwisowe prowadzone na sprzęcie Urzędu w jego siedzibie lub w siedzibie serwisu, muszą być potwierdzone notatką lub wpisem do dziennika opisującym czas, datę rozpoczęcia i zakończenia prac, zakres prac oraz osoby prowadzące prace
f) Prowadzenie prac w trybie zdalnym odbywać się może jedynie za zgodą osoby upoważnionej lub Administratora Systemów Informatycznych. Pracownik, który chce udostępnić połączenie dla firm serwisujących oprogramowanie, może to zrobić jedynie po otrzymaniu pisemnej zgody (np. e-mail). Dla każdego połączenia musi być sporządzona notatka lub wpis do dziennika systemu informatycznego, zawierający informacje o:
    - Czasie trwania prac

- Ich zakresie
- Osobie prowadzącej serwis
- Osobie udostępniającej zdalny dostęp

Udostępnianie połączenia w trybie zdalnym może odbywać się jedynie w godzinach pracy Urzędu.

10. Dokumenty i zapisy

Załącznik nr 1 – Upoważnienie do przetwarzania danych osobowych

Załącznik nr 2 – Oświadczenie o zapoznaniu się z obowiązującymi przepisami

Załącznik nr 3 – Karta uprawnień użytkownika systemu informatycznego

Załącznik nr 4 – Wykaz osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 5 – Wniosek o nadanie/cofnięcie uprawnień do przetwarzania danych osobowych

Wyżej wymienione dokumenty i formularze stanowią załączniki do IZSI. Zarządzanie nimi odbywa się zgodnie z zasadami przyjętymi dla dokumentacji systemowej.

Załącznik nr 1
do Instrukcji Zarządzania
Systemami Informatycznymi
w Urzędzie Gminy Srokowo

Upoważnienie do przetwarzania danych osobowych

miejscowość, dnia ……..

(nazwa jednostki)

Upoważnienie nr…./….

do przetwarzania danych osobowych

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922 ze zm.)

Upoważniam Pana/Panią:

……..

do przetwarzania danych osobowych

w Urzędzie Gminy Srokowo, w zakresie niezbędnym do działania

…….
(*nazwa komórki organizacyjnej*)
– określonym w *Regulaminie organizacyjnym Urzędu Gminy Srokowo* lub danych przetwarzanych w następujących zbiorach danych:

1. ……..
2. ……..
3. ……..

Upoważnienie jest ważne na czas zatrudnienia w komórce organizacyjnej/Upoważnienie jest ważne do dnia...../Upoważnienie jest ważne przez okres wykonywania zadania ……. (jakiego – do kiedy?)
* (*niepotrzebne skreślić*)

…….
pieczęć i podpis osoby nadającej upoważnienie

Załącznik nr 2
do Instrukcji Zarządzania
Systemami Informatycznymi
w Urzędzie Gminy Srokowo

Oświadczenie o zapoznaniu się z obowiązującymi przepisami

Srokowo, dnia ……..

……..
(imię i nazwisko upoważnionego)

……..
(stanowisko lub funkcja)

……..
(komórka organizacyjna lub nazwa podmiotu)

Oświadczam, że przed przystąpieniem do pracy przy przetwarzaniu danych osobowych zostałam/em zaznajomiona/ny z przepisami dotyczącymi ochrony danych osobowych, w tym z Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2016 r., poz. 922) oraz rozporządzeniami wykonawczymi wydanymi na jej podstawie.

Zapoznałam/em się również z zasadami dotyczącymi bezpieczeństwa i ochrony informacji opisanymi w:

a) Polityce Bezpieczeństwa i Ochrony Danych Osobowych w Urzędzie Gminy Srokowo
b) Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Gminy Srokowo

i zobowiązuję się do przestrzegania zasad wynikających z ich treści.

W związku z realizowanymi zadaniami i pełnionymi funkcjami w Urzędzie Gminy Srokowo zobowiązuję się do:

a) Zachować w tajemnicy dane, w tym dane osobowe do przetwarzania których zostałam/em upoważniona/y
b) Zachować w tajemnicy chronione informacje Urzędu Gminy Srokowo, do których miałam/em dostęp w związku z pełnionymi funkcjami
c) Zachować w tajemnicy sposoby zabezpieczenia danych osobowych oraz informacji chronionych
d) Zapoznać się z aktualizacjami funkcjonującej dokumentacji oraz nowymi dokumentami dotyczącymi bezpieczeństwa informacji i przestrzegać zasad z nich wynikających

Przyjmuję do wiadomości:

a) Sieć LAN Urzędu Gminy Srokowo oraz wszelki ruch LAN/WAN jest pod stałym monitoringiem Administratora Systemu Informatycznego.

Zobowiązanie do zachowania tajemnicy jest w mocy zarówno w trakcie pracy, realizowania zadań na rzecz Urzędu Gminy Srokowo, jak i po ich zakończeniu. Przyjmuję do wiadomości, iż Urząd Gminy Srokowo zgodnie z obowiązującym prawem może bezterminowo pociągnąć mnie do odpowiedzialności w przypadku rażącego naruszenia zobowiązania.

……..
(Data i podpis upoważnionego)

Załącznik nr 3
do Instrukcji Zarządzania
Systemami Informatycznymi
w Urzędzie Gminy Srokowo

Karta uprawnień użytkownika systemu informatycznego

Karta uprawnień użytkownika do systemu informatycznego

1. Dane użytkownika

Imię i nazwisko	
Stanowisko	
Numer pokoju	

2. Cel

	Rejestracja nowego użytkownika
	Aktualizacja uprawnień lub danych użytkownika
	Zawieszenie dostępu
	Przywrócenie zawieszonego dostępu
	Usunięcie użytkownika

3. Rodzaj uprawnień

	Administrator
	Użytkownik

4. Ograniczenie uprawnień

	Nazwa systemu	Nazwa modułu
	System operacyjny	
	PUMA	Administracja
	PUMA	Budżet
	PUMA	Decyzje
	PUMA	Eksport Danych
	PUMA	EPG
	PUMA	Ewidencja Ludności
	PUMA	FK
	PUMA	Import danych geodezyjnych
	PUMA	Kadry
	PUMA	Kasa
	PUMA	Koncesje alkoholowe
	PUMA	Kontrahenci
	PUMA	OPJ – Podatek od osób prawnych
	PUMA	Płace
	PUMA	Podatki
	PUMA	Podatki os. fizyczne
	PUMA	POST
	PUMA	Statystyki dla Rejestru Mieszkańców
	PUMA	Symulacje
	PUMA	Szablony i archiwum wydruków
	PUMA	Środki trwałe

	PUMA	Urząd Stanu Cywilnego
	PUMA	Windykacja
	PUMA	Wyborcy
	PUMA	Zaświadczenia
	Płatnik	
	ePFRON	
	EWOPIS	
	EWMAPA	
	SIO stare	
	SIO nowe	
	Bestia	
	Poczta e-mail	
	Cyfrowy Urząd	
	e-PUAP	
	CEIDG	
	LEX	
	SRPP	
	Urzędowa Poczta Elektroniczna	Publikacja uchwał w Dzienniku Urzędowym
	Urząd Zamówień Publicznych	Publikacja przetargów
	Strona Internetowa	
	BIP	
	Platforma Wyborcza	
	Rejestr Pełnomocnictw Ogólnych	
	System Bankowy	
	SRP	Dowody Osobiste
	SRP	USC
	SRP	PESEL
	SRP	Administrator
	Punkty Adresowe iMPA	Administrator
	Punkty Adresowe iMPA	Użytkownik
	iSRB	
	Shrimp	
	Portal sprawozdawczy GUS	

……
(Data i podpis ASI)

……
(Data i podpis ADO)

Załącznik nr 4
do Instrukcji Zarządzania
Systemami Informatycznymi
w Urzędzie Gminy Srokowo

Wykaz osób upoważnionych do przetwarzania danych osobowych

Nr	Nazwa systemu/modułu	Nr	Nazwa systemu/modułu
1	System operacyjny	**29**	EWOPIS
2	PUMA - Administracja	**30**	EWMAPA
3	PUMA - Budżet	**31**	SIO stare
4	PUMA - Decyzje	**32**	SIO nowe
5	PUMA - Eksport Danych	**33**	Bestia
6	PUMA - EPG	**34**	Poczta e-mail
7	PUMA - Ewidencja Ludności	**35**	Cyfrowy Urząd
8	PUMA - FK	**36**	e-PUAP
9	PUMA - Import danych geodezyjnych	**37**	CEIDG
10	PUMA - Kadry	**38**	LEX
11	PUMA - Kasa	**39**	SRPP
12	PUMA - Koncesje alkoholowe	**40**	Urzędowa Poczta Elektroniczna
13	PUMA - Kontrahenci	**41**	Urząd Zamówień Publicznych
14	PUMA - OPJ – Podatek od osób prawnych	**42**	Strona Internetowa
15	PUMA - Płace	**43**	BIP
16	PUMA - Podatki	**44**	Platforma Wyborcza
17	PUMA - Podatki os. fizyczne	**45**	Rejestr Pełnomocnictw Ogólnych
18	PUMA - POST	**46**	System Bankowy
19	PUMA - Statystyki dla Rejestru Mieszkańców	**47**	SRP - Dowody Osobiste
20	PUMA - Symulacje	**48**	SRP - USC
21	PUMA - Szablony i archiwum wydruków	**49**	SRP - PESEL
22	PUMA - Środki trwałe	**50**	SRP - Administrator
23	PUMA - Urząd Stanu Cywilnego	**51**	Punkty Adresowe iMPA – Administrator
24	PUMA – Windykacja	**52**	Punkty Adresowe iMPA – Użytkownik
25	PUMA – Wyborcy	**53**	iSRB
26	PUMA – Zaświadczenia	**54**	Shrimp
27	Płatnik	**55**	UKE Teleinfrastruktura
28	ePFRON	**56**	Portal sprawozdawczy GUS

U – użytkownik **A – administrator**

Lp	Imię i nazwisko	Numer upoważnienia	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	System Informatyczny / nadany identyfikator użytkownika (login)
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						

Załącznik nr 5
do Instrukcji Zarządzania
Systemami Informatycznymi
w Urzędzie Gminy Srokowo

Wniosek o nadanie/cofnięcie uprawnień do przetwarzania danych osobowych

Srokowo, dnia ……..

Wniosek
o nadanie/cofnięcie uprawnień do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922) wnoszę o nadanie/cofnięcie uprawnień dla

Pani/Pana

……

Pracownika

……

……

……

……

do wykonywania czynności związanych z przetwarzaniem danych osobowych w zakresie:

……

……

……

na okres od ..... **do** .....

.....
(podpis Administratora Danych Osobowych)