Załącznik nr 2
do Zarządzenia nr 13/17
Wójta Gminy Duszniki
z dnia 2 marca 2017 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Duszniki

§1

Postanowienia ogólne

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Urzędu Gminy Duszniki, 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.
2. Niniejsza instrukcja realizuje „Politykę bezpieczeństwa Urzędu Gminy Duszniki".

§2

Podstawa prawna

Podstawą prawną są § 3 i 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w 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

Definicje

Ilekroć mowa w niniejszym dokumencie o:

1. Instrukcji, należy przez to rozumieć "Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Duszniki".
2. Polityce, należy przez to rozumieć "Politykę bezpieczeństwa Urzędu Gminy Duszniki".
3. Urzędzie należy przez to rozumieć Urząd Gminy Duszniki.
4. Administratorze Bezpieczeństwa Informacji (ABI) - należy przez to rozumieć pracownika wyznaczonego przez Administratora Danych - Wójta Gminy Duszniki do nadzorowania przestrzegania zasad ochrony danych osobowych.
5. Lokalni Administratorzy Bezpieczeństwa Informacji (LABI) - należy przez to rozumieć kierowników poszczególnych referatów w Urzędzie Gminy Duszniki.

6. Administrator Systemu Informatycznego - osoba wyznaczona przez administratora, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, i techniczne bezpieczeństwo przetwarzania danych w sieci informatycznej. Dopuszcza się powierzenie funkcji ASI osobie lub firmie zewnętrznej o udokumentowanym doświadczeniu w wykonywaniu czynności przypisanych do Administratora Systemu Informatycznego.
7. Użytkowniku systemu - należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie.

§4

Procedury nadawania i zmiany uprawnień do przetwarzania danych.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
   a) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r.,poz. 922) oraz aktami wykonawczymi do powyższej ustawy,
   b) Polityką bezpieczeństwa Urzędu Gminy Duszniki,
   c) niniejszym dokumentem,

   oraz posiadać upoważnienie do przetwarzania danych osobowych.
2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 1 do Polityki bezpieczeństwa.
3. Administrator Systemu Informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego. Zakres uprawnień odpowiada uzyskanemu upoważnieniu do przetwarzania danych osobowych.
4. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego loginu, hasła oraz zakresu dostępnych danych i operacji.
5. Hasło ustanowione podczas przyznawania uprawnień przez Administratora Systemu Informatycznego należy zmienić na indywidualne podczas pierwszego logowania się w systemie.
6. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
7. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
8. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe na poziomie dostępu do systemu operacyjnego i sieci lokalnej oraz dostępu do poszczególnych aplikacji służących do przetwarzania danych osobowych.
9. Odebranie uprawnień pracownikowi następuje na pisemny wniosek Wójta Gminy Duszniki z podaniem daty odebrania uprawnień.
10. Wójt Gminy Duszniki informuje pisemnie Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej pracowników, mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
11. Należy niezwłocznie zablokować dostęp do systemu informatycznego poprzez unieważnienie loginu i hasła użytkownikowi, który utracił uprawnienia do dostępu do danych osobowych.
12. Administrator Danych Osobowych jest zobowiązany do prowadzenia i ochrony ewidencji osób upoważnionych i ich uprawnień. Wzór rejestru stanowi załącznik nr 4 do Polityki.

§5

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

1. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu loginu **i** hasła.
2. Hasło dostępu powinno być zmieniane przez użytkownika co najmniej raz w miesiącu.
3. Login użytkownika nie może być zmieniany bez wyraźnej przyczyny, a po utracie uprawnień przez użytkownika z systemu informatycznego nie może zostać przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich loginów i haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, należy natychmiast zmienić hasło i poinformować o zaistniałym fakcie Administratora Bezpieczeństwa Informacji.
7. Minimalna długość hasła zawiera 8 znaków.
8. Hasło powinno zawierać przynajmniej jedną dużą literę, jedną cyfrę oraz jeden znak specjalny (.,();'@, #, & itp.), o ile możliwe jest zastosowanie tych reguł w systemie informatycznym i aplikacjach.
9. Zmiany hasła dokonuje użytkownik systemu.
10. Nie wolno zlecać zmiany hasła innym osobom.

§6

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

1. Przed rozpoczęciem pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych. W przypadku ich wykrycia należy niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.
2. W celu rozpoczęcia pracy użytkownik wykonuje logowanie do systemu używając indywidualnego loginu i hasła.
3. Podczas nieobecności przy stanowisku komputerowym należy wylogować się z sytemu bądź uruchomić wygaszacz ekranu chroniony hasłem.
4. Po zakończeniu pracy w systemie należy zakończyć prace aplikacji, wylogować się z systemu i wyłączyć stację roboczą.
5. Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo (np. w celu konserwacji sprzętu). Planowe zawieszenie prac jest uprzedzone informacją do pracowników Urzędu (w formie wiadomości email lub osobiście) przez Administratora Systemu Informatycznego na co najmniej 10 minut przed planowanym zawieszeniem.

§7

Procedury tworzenia kopii zapasowych.

1. Kopie bezpieczeństwa danych umieszczonych na serwerach wykonywane są codziennie poprzez systemy archiwizowania centralnego - wskazane w Polityce bezpieczeństwa.
2. Kopie bezpieczeństwa indywidualnych/personalnych danych użytkownika oraz danych zapisywanych w programach, których bazy danych znajdują się na zasobach lokalnych wykonują pracownicy obsługujący te programy poprzez skopiowanie danych na dedykowany danemu użytkownikowi dysk sieciowy. Kopie wykonuje się codziennie, chyba że użytkownik w danym dniu nie zmieniał danych zapisanych w bazie. Za częstotliwość wykonywania kopii bezpieczeństwa lokalnych danych odpowiada użytkownik.
3. Dodatkowe zabezpieczenie wszystkich programów i danych wykonywane jest nie rzadziej niż raz w miesiącu poprzez zapis na dyskach zewnętrznych, przechowywanych w szafie metalowej w pokoju nr 6 Urzędu. Osobą odpowiedzialną za wymianę kopii awaryjnych na aktualne jest Skarbnik lub osoba wyznaczona przez Skarbnika.
4. Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza Administrator Systemu Informatycznego.

§8

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków.

1. Elektroniczne nośniki informacji.

a) Dane osobowe w postaci elektronicznej - za wyjątkiem kopii bezpieczeństwa - nie mogą opuścić obszaru przetwarzania danych osobowych.

b) Elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa, w zamkniętych szafach lub metalowych kasetach.

c) Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a następnie uszkadza się w sposób mechaniczny.

d) Elektroniczne nośniki informacji, zawierające dane osobowe, nie mogą zostać przekazane innemu podmiotowi nieuprawnionemu do dostępu do tych danych, nawet po uprzednim usunięciu danych z nośnika.

e) Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

2. Kopie zapasowe.

a) Kopie bezpieczeństwa są przechowywane w szafie w pokoju nr 6 Urzędu Gminy Duszniki oraz w Serwerowni Urzędu Gminy Duszniki.

b) Dostęp do danych opisanych w punkcie 1 ma Administrator Systemu Informatycznego oraz upoważnieni pracownicy.

3. Wydruki.

a) W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.

b) Pomieszczenie, w którym przechowywane są wydruki robocze, musi być należycie

zabezpieczone po godzinach pracy.

c) Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§9

Zabezpieczenia

1. Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwerów i stacji roboczych, na których przetwarzane są dane osobowe zapewniają zasilacze UPS.
2. Do logowania się w systemie stosowane są hasła.
3. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień.
4. Niniejsza instrukcja zawiera opis stosowanych metod i środków uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.
5. Stosuje się aktywną ochronę antywirusową serwerów i stacji roboczych. Program antywirusowy aktualizuje się automatycznie codziennie.
6. Bezwzględnie zabrania się używania nośników niewiadomego pochodzenia.
7. Bezwzględnie zabrania się pobierania z sieci Internet plików niewiadomego pochodzenia.
8. W przypadku wykrycia szkodliwego oprogramowania sprawdzane jest stanowisko komputerowe, na którym wykryto wirusa oraz wszystkie posiadane przez użytkownika nośniki.

§10

Procedury związane z oprogramowaniem.

1. Pracownicy Urzędu Gminy Duszniki mogą wykorzystywać jedynie legalne oprogramowanie zainstalowane za zgodą Administratora Systemu Informatycznego.
2. Instalacja oprogramowania na stanowiskach pracowniczych może być dokonywana tylko i wyłącznie z nośników znajdujących się w zasobach Urzędu.
3. Za zgodą Administratora Danych Osobowych decyzje o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych podejmuje Administrator Sytemu Informatycznego.
4. Administrator Systemu Informatycznego po wydaniu zgody na instalację oprogramowania, zobowiązany jest do zaktualizowania metryki odpowiedniego komputera lub stanowiska pracy oraz do zinwentaryzowania ewentualnej dokumentacji i nośników instalacyjnych potwierdzających legalność danego programu.
5. Nośniki instalacyjne oprogramowania znajdują się na serwerze zasobów lub w zamkniętej szafie, do której dostęp mają jedynie upoważnione osoby. Nośniki nie mogą się być przechowywane w żadnym innym miejscu, nie wolno ich kopiować, wypożyczać lub przekazywać osobom trzecim w żadnej formie.
6. Każdy z pracowników zobowiązany jest do podpisania metryki komputera, na której wymienione jest oprogramowanie, które jest zainstalowane na jego stanowisku pracy.
7. Wszyscy pracownicy zobowiązują się do przestrzegania wymogu pracy wyłącznie na oprogramowaniu wymienionym w metryce komputera.

8. Zabrania się wnoszenia na teren urzędu prywatnych kopii oprogramowania i plików multimedialnych oraz pobierania i kopiowania z Internetu wszelkich utworów (programów komputerowych, utworów muzycznych, filmów, gier komputerowych, itp.), będących przedmiotem ochrony praw autorskich.
9. Konieczne zakupy oprogramowania lub instalowanie oprogramowania nie będącego w zasobach urzędu muszą być uzgadniane i konsultowane z Administratorem Systemu Informatycznego.
10. W celu zwiększenia bezpieczeństwa użytkowanego oprogramowania Urząd Gminy Duszniki korzysta z systemu Statlook, który służy do monitorowania legalności zainstalowanego oprogramowania oraz wszystkich procesów zachodzących na kontrolowanym komputerze. System rejestruje wszystkie operacje realizowane na monitorowanym komputerze i umożliwia bieżący podgląd czynności wykonywanych na komputerze.
11. Wszelkie wątpliwości dotyczące instalacji i użytkowania oprogramowania oraz korzystania z plików multimedialnych, rozstrzygane są przez Administratora Systemu Informatycznego.
12. Każde złamanie wyżej wymienionych ustaleń, ze względu na obowiązujące przepisy prawne, stanowi poważne naruszenie zasad pracy.
13. Zezwala się pracownikom na korzystanie z przenośnego komputera służbowego poza miejscem pracy, pod warunkiem przestrzegania zasad określonych w Polityce bezpieczeństwa i w niniejszej instrukcji.

§11

Procedury wykonywania przeglądów i konserwacji systemu.

1. Przeglądy i konserwacja urządzeń.
   a) Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.
   b) Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji.
2. Przegląd programów i narzędzi programowych.
   a) Konserwacja baz danych osobowych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.
   b) Administrator Systemu Informatycznego sprawuje :
      - nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe,
      - nadzór nad wykonywaniem kopii zapasowych i ich przechowywaniem,
   c) Administrator Systemu Informatycznego zobowiązany jest uaktywnić mechanizm zliczania nieudanych prób dostępu do systemu oraz ustawić blokadę konta użytkownika po wykryciu ustalonej liczby nieudanych prób, we wszystkich systemach posiadających taką funkcję.
3. Rejestracja działań konserwacyjnych, awarii oraz napraw.
   a) Administrator Systemu Informatycznego prowadzi "Rejestr systemu informatycznego".
   b) „Rejestr systemu informatycznego” stanowi zbiór kopii protokołów zdawczo-odbiorczych spisywanych na koniec wykonywanych prac.

§12

Współpraca z firmą zewnętrzną zajmującą się konserwacją systemu informatycznego oraz naprawą sprzętu komputerowego.

1. Zasady współpracy określa umowa zawarta pomiędzy Gminą Duszniki a firmą zewnętrzną.
2. Umowa obejmuje klauzulę dotyczącą ochrony danych osobowych.
3. Osobą odpowiedzialną za kontakty z firmą jest Administrator Systemu Informatycznego.
4. Administrator Systemu Informatycznego może powierzyć wykonanie prac wskazanych w niniejszej instrukcji pracownikowi firmy zewnętrznej.
5. Administrator Systemu Informatycznego lub osoba przez niego wyznaczona nadzoruje wykonywanie prac przez pracowników firmy zewnętrznej, ze szczególnym uwzględnieniem możliwości naruszenia zasad ochrony danych osobowych.
6. Po zakończeniu prac sporządzany jest protokół odbioru, a zakres prac wpisywany jest do rejestru, o którym mowa w §11.

§13

Postanowienia powyższej instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych mają również zastosowanie do zarządzania pozostałym systemem informatycznym Urzędu, niezwiązanym z przetwarzaniem danych osobowych.