Załącznik Nr 2 do Zarządzenia Nr. 144 / 2015 z dnia 17 grudnia 2015 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
w
URZĘDZIE MIASTA I GMINY
W MAŁOGOSZCZU

Rozdział 1.

Postanowienia ogólne

§ 1

Instrukcja zarządzania systemem informatycznym zwana dalej instrukcją, jest dokumentem regulującym zasady oraz procesy zarządzania i administrowania Systemami Informatycznymi Urzędu Miasta i Gminy w Małogoszczu, w celu bezpiecznego ich przetwarzania.

§ 2

1. Instrukcja określa ogólne zasady i tryb postępowania Administratora Danych oraz wszystkich użytkowników przetwarzających dane osobowe w systemie informatycznym Urzędu Miasta i Gminy w Małogoszczu
2. Podstawę prawna:
    a. Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych - tekst jednolity (j.t Dz.U. z 2014 poz. 1182 ze zm).
    b. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

§ 3

Określenia i skróty użyte w instrukcji oznaczają:

1. **Urząd** - Urząd Miasta i Gminy w Małogoszczu
2. **Administrator Danych Osobowych - Burmistrz Miasta i Gminy w Małogoszczu** zwany dalej **ADO.**
3. **Administrator Bezpieczeństwa Informacji** - pracownik urzędu lub inna osoba wyznaczona przez ADO, do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie, oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych, zwana dalej **ABI.**
4. **Administrator Systemów Informatycznych,** zwany dalej **ASI** - osoba odpowiedzialna za funkcjonowanie systemu informatycznego urzędu oraz stosowanie technicznych

i organizacyjnych środków ochrony i zabezpieczeń przewidzianych w systemach informatycznych.

5. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych
6. **Bezpieczeństwo systemu informatycznego** - wdrożenie przez ADO lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.
7. **Dane osobowe-** wszelkie informacje w wersji tradycyjnej i elektronicznej dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
8. **Zbiór danych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnym wg określonych kryteriów
9. **Przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
10. **Osoba upoważniona lub użytkownik systemu** - osoba posiadająca upoważnienie wydane przez ADO lub uprawnioną przez niego osobę i dopuszczona jako użytkownik do przetwarzania danych
    osobowych w systemie informatycznym danej komórki organizacyjnej, zwana dalej **użytkownikiem.** Użytkownikiem może być pracownik urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w urzędzie
11. **Przełożony użytkownika** - kierownik, osoba odpowiedzialna za przestrzeganie zasad przetwarzania i ochrony danych przez podległych mu pracowników
12. **Osoba uprawniona** - osoba posiadająca upoważnienie wydane przez ADO do wykonywania w jego imieniu określonych czynności.

Rozdział II

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

§ 4

1. Każdy pracownik Urzędu zobowiązany jest zapoznać się z ustawą o ochronie danych osobowych, polityką bezpieczeństwa i niniejszą instrukcją i stosować jej przepisy na swoim stanowisku pracy

2. Przetwarzania danych osobowych może dokonywać jedynie użytkownik systemu upoważniony przez ADO i ma prawo do wykonywania tylko tych czynności, do których został upoważniony - karta nadania/cofnięcia uprawnień załącznik Nr 1
3. Ewidencję uprawnień w zakresie dostępu do systemu informatycznego dokonuje ASI na podstawie otrzymanej karty nadania/ cofnięcia dostępu, załącznik Nr 2
4. Nadużycie przez użytkownika systemu postanowień niniejszej Instrukcji, może stanowić podstawę do pociągnięcia go do odpowiedzialności przewidzianej właściwymi przepisami prawa.
5. Użytkownik systemu , który przetwarza dane osobowe zobowiązany jest do zachowania tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.
6. Odebranie uprawnień użytkownikowi systemu następuje w oparciu pismo ABI zawierające datę i przyczynę : min

   - w związku ze zmianą zakresu zadań
   - w związku z zakończeniem stosunku pracy, zadania wynikającego z umowy cywilnoprawnej, stażu
   - inną utratą uprawnień

§ 5

Naczelną zasadą bezpieczeństwa systemu informatycznego jest ochrona informacji przed nieuprawnionym dostępem, ujawnieniem, przypadkowym lub nieautoryzowanym zniszczeniem lub modyfikacją danych. Stosowanie zasad uwierzytelniania użytkowników ma podstawowy wpływ na zachowanie poufności, rozliczalności oraz integralności danych

§ 6

1. Dla każdego użytkownika systemu podczas przyznawania uprawnień ASI ustala identyfikator i hasło Ustanowione hasło ASI przekazuje użytkownikowi systemu formie pisemnej lub ustnej
2. W systemie informatycznym stosowane jest uwierzytelnienie użytkownika przy pomocy jego identyfikatora i hasła. Stosowanie unikalnego identyfikatora realizuje zasadę rozliczalności użytkowników systemu informatycznego. Identyfikator użytkownika składa się z 6 znaków, z których dwa pierwsze odpowiadają literom imienia a cztery kolejne odpowiadają pierwszym literom nazwiska. W identyfikatorze pomija się polskie znaki diaktryczne
3. Hasło należy zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym. System automatycznie powinien wymuszać zmianę hasła

4. W celu zapewnienia wysokiego poziomu bezpieczeństwa hasło musi zawierać co najmniej 8 znaków i zawierać jednocześnie duże i małe litery oraz cyfry lub znaki specjalne.
5. Użytkownik systemu utrzymuje hasło w tajemnicy- również po upływie jego ważności. Jest odpowiedzialny za zachowanie poufności swoich haseł i powinien wprowadzać hasło w taki sposób, który uniemożliwia innym osobom jego poznanie .
6. Hasło jest wpisywane i przechowywane w systemie informatycznym w postaci zaszyfrowanej.
7. Hasło użytkownika systemu musi być zmienianie nie rzadziej niż raz na 30 dni. W przypadku gdy użytkownik systemu informatycznego nie korzysta z danego systemu przez okres dłuższy niż 30 dni hasło musi zostać zmienione podczas najbliższego ponownego zalogowania.
8. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.
9. Hasło użytkownika systemu, który utracił uprawnienia dostępu do danych osobowych unieważnia się bezzwłocznie oraz podejmuje inne niezbędne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych
10. Osobą odpowiedzialną za prawidłowe funkcjonowanie mechanizmów zawartych w § 6 jest ASI.
11. Użytkownik systemu ponosi odpowiedzialność za czynności wykonane w systemie przy użyciu identyfikatora i hasła, którymi się posługuje i zobowiązany jest do utrzymania haseł dostępu w tajemnicy a w szczególności do dołożenia wszelkich starań w celu uniemożliwienia zapoznania się z nimi osób trzecich nawet po ustaniu ich ważności.
12. Identyfikator użytkownika systemu, która utraciła uprawnienia do dostępu danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.

§ 7

1 .ASI prowadzi „Ewidencję użytkowników systemu osób posiadających uprawnienia do przetwarzania „danych osobowych", która zawiera:

- imię i nazwisko użytkownika
- zakres uprawnień
- nazwę identyfikatora
- datę zarejestrowania w systemie
- datę wyrejestrowania z systemu

2.Jakakolwiek zmiana informacji wyszczególnionych w ewidencji podlega natychmiastowemu odnotowaniu.

Rozdział III

Procedury rozpoczęcia, zawieszenia, zakończenia pracy systemie informatycznym

§ 8

1. Użytkownik systemu rozpoczynający pracę zobowiązany jest przestrzegać procedur, które mają na celu sprawdzenie zabezpieczenia pomieszczenia w którym przetwarzane są dane osobowe, swojego stanowiska pracy oraz stanu sprzętu komputerowego.
2. Użytkownik systemu przed przystąpieniem do przetwarzania danych powinien zalogować się w systemie, posługując się swoim identyfikatorem i hasłem.
3. Użytkownik systemu w czasie pracy powinien stosować przedsięwzięcia zapewniające bezpieczeństwo przetwarzania danych osobowych w systemie:
    - ustawić ekrany monitorów w pomieszczeniach tak, aby uniemożliwić podgląd osobom nieuprawnionym
    - w przypadku przekroczenia 10 minut braku aktywności następuje automatyczna blokada systemu bądź automatyczny wygaszacz ekranu chroniony hasłem.
4. Przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane informacje lub dane poprzez zabezpieczenie komputera lub wylogowanie się z systemu.
5. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji (płyty CD, dyskietki, pamięci usb, itp.)
6. Użytkownik w pełnym zakresie odpowiada za powierzony sprzęt komputerowy i wykonywane czynności aż do momentu rozliczenia ze sprzętu komputerowego.

Rozdział IV
Procedury tworzenia kopii zapasowych

§ 9

1. W urzędzie stosowana jest praktyka przetwarzania danych w bazach danych na dedykowanych dla systemu informatycznego serwerach.
2. Kopie zapasowe baz danych zlokalizowanych na serwerach wykonywane są w cyklach:
    - w cyklu dobowym(w godzinach nocnych) za pomocą programów archiwizujących tworzone są pełne kopie baz danych
    - w cyklu tygodniowym -tworzone są kopie aplikacji
    - w cyklu podyktowanym potrzebami własnymi urzędu oraz przepisami prawa

3. W przypadku braku technicznych możliwości sporządzenia kopii zgodnie z planem, należy je wykonać w najbliższym możliwym terminie.
4. Kopie zapasowe tworzone są na macierzy danych .
5. Kopiami zapasowymi, zgodnie z rozporządzeniem zabezpiecza się zarówno dane jak i programy służące do ich przetwarzania.
6. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada ASI
7. Użytkownicy systemu we własnym zakresie odpowiadają za sporządzanie kopii zapasowych i awaryjnych wytworzonych przez siebie dokumentów i danych znajdujących się na lokalnych dyskach twardych wykorzystywanych przez nich stacji roboczych. Jednocześnie mają obowiązek dopilnowania, aby dane przetwarzane przy pomocy oprogramowania nie przeznaczonego do przetwarzania danych osobowych bądź też oprogramowania służącego przetwarzaniu danych osobowych wyłącznie w celu ich udostępnienia na piśmie, i zapisywane na nośnikach informatycznych nie zawierały danych osobowych.

Rozdział V

Sposób, miejsce i czas przechowywania elektronicznych nośników informacji (w tym kopii zapasowych)

1. Dane w postaci elektronicznej przetwarzane w systemie zapisane na dyskietkach, dyskach, taśmach, dyskach twardych są własnością urzędu
2. Wymienne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych określony w Polityce Bezpieczeństwa. Po zakończeniu pracy przez użytkowników systemu nośniki te są przechowywane w zamykanych szafach biurowych.
3. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy jest to możliwe uszkadza w sposób uniemożliwiający ich odczytanie.
4. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych.
5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do naprawy pozbawia się wcześniej zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej
6. Kopii awaryjnych wykonywanych na nośnikach magnetycznych nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco. Przechowuje się je w miejscach zabezpieczonych przed nieuprawnionym przejęciem, modyfikacji), uszkodzeniem lub zniszczeniem.

7. Kopie awaryjne należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu.
8. Kopie awaryjne usuwane są niezwłocznie po ustaniu ich użyteczności

Rozdział VI
Sposób zabezpieczenia systemu informatycznego -środki ochrony

§ 11

1. W celu zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych należy zastosować środki bezpieczeństwa na poziomie wysokim.
2. Za ochronę antywirusową odpowiada ASI, który wykonuje związane z tym czynności wykorzystując moduły programu antywirusowego w aktualnej wersji - program, sprawdzające bieżąco zasoby systemu informatycznego. Program antywirusowy powinien automatycznie sygnalizować obecność wirusów oraz niebezpiecznego oprogramowania ułatwiającego zdalny dostęp do informacji oraz posiadać mechanizmy uaktualniania bazy danych wirusów
3. Oprogramowanie antywirusowe jest instalowane na serwerze oraz na wszystkich stanowiskach komputerowych podłączonych do systemu informatycznego.
4. Aktualizacja oprogramowania antywirusowego odbywa się automatycznie dla wszystkich zainstalowanych aplikacji nie rzadziej niż raz w tygodniu.
5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia.
6. O każdorazowym wykryciu wirusa użytkownik zobowiązany jest niezwłocznie powiadomić ASI, który dokonuje analizy problemu i podejmuje stosowne działania naprawcze.
7. Dodatkowo należy zastosować sprzętowe urządzenie oddzielające sieć komputerową od bezpośredniego dostępu do Internetu, typu zarządzany router, stanowiące blokadę przed nieuprawnionym dostępem z zewnątrz do systemu informatycznego urzędu.
8. W sytuacji konieczności podłączenia do systemu komputerowego nośnika informacji pochodzącego z zewnętrznego źródła (np. płyty cd/dvd, pamięci usb itp.) nośnika taki musi zostać poddany weryfikacji pod kątem infekcji szkodliwym oprogramowaniem przez ASI Zabrania się używania do codziennej pracy urządzeń pamięci masowej nie będących na wyposażeniu Urzędu i nie zatwierdzonych przez ASI. 9. Zabrania się używania i wynoszenia urządzeń i nośników informacji wykorzystywanych do pracy w Urzędzie poza obszar przetwarzania danych. W przypadku zaistnienia takiej konieczności należy uzyskać zgodę ADO/ABI. Jeśli nośnik danych umożliwiający zapis (dyskietka, pamięć USB itp.) został podłączony do zewnętrznego urządzenia (np. komputer domowy, stacja robocza w jednostce podległej itp.) przed jego ponownym podłączeniem do systemu informatycznego Urzędu musi zostać poddany weryfikacji jak w pkt 6.

§12

Wymagania które powinien spełniać system informatyczny służący do przetwarzania 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 systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba
    c) źródła danych w przypadku zbierania danych, nie od osoby, której one dotyczą
    d) 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
    e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

Rozdział VII

Sposób dokonywania przeglądów i konserwacji systemu oraz zbiorów danych osobowych

§13

1. Okresowe oraz bieżące przeglądy i konserwacje sprzętu komputerowego, wynikające z eksploatacji, warunków zewnętrznych oraz ważności systemu dla funkcjonowania Urzędu Miasta i Gminy w Małogoszczu wykonuje ASI. Powinny być one wykonane w terminach określonych przez producenta sprzętu.
2. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do naprawy w firmach zewnętrznych, pozbawia się przed naprawą zapisu danych osobowych, albo naprawia je pod nadzorem ASI.
3. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do likwidacji należy pozbawić zapisu, a w przypadku gdy jest to niemożliwe uszkodzić mechanicznie w sposób uniemożliwiający ich odczytanie.

4. Przegląd programów i narzędzi programowych - konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.
5. 5. ASI zobowiązany jest uaktywnić mechanizm zaliczania nieudanych prób zameldowania do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób we wszystkich systemach posiadających taka funkcję.

§14

Postępowanie w przypadku przekazywania nośników z danymi osobowymi poza obszar przetwarzania danych.

1**.** Dane osobowe zapisane na urządzeniach i nośnikach informacji, o których mowa w art. 27 ust.] ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przekazywane poza obszar przetwarzania danych osobowych, w celu zapewnienia ich poufności i integralności powinny wcześniej zostać zakodowane stosownym programem przy użyciu co najmniej 8 literowego hasła, które musi zawierać duże i małe litery oraz cyfry lub znaki specjalne.

Rozdział VIII

§ 15

Postanowienia końcowe.

1. Użytkownik systemu informatycznego nie ma prawa dokonywania samodzielnych instalacji, deinstalacji jakiegokolwiek oprogramowania, ani wprowadzania zmian w konfiguracji oprogramowania wykraczających poza jego normalne użytkowanie.
2. Czynności o których mowa w § **15 pkt 1** wykonuje ASI.
3. ABI prowadzi „Rejestr zbiorów danych osobowych przetwarzanych w systemach informatycznych"
4. ASI przeprowadza szkolenia dla nowozatrudnionych pracowników oraz w przypadku istotnych zmian w systemach informatycznych, w których przetwarzane są dane osobowe z zakresu stosowania Instrukcji Zarządzania Systemem Informatycznym.
5. ABI dokonuje okresowego sprawdzenia sprawności funkcjonowania zabezpieczeń systemów w których przetwarzane są dane osobowe.

§16

W sprawach nieuregulowanych niniejszą Instrukcją zastosowanie znajdują przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych - tekst jednolity (j.t Dz.U. z 2014 poz. 1182 ze zm.i rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. (DZ. U. Nr 100, poz. 1024)

Załącznik Nr 1
do Instrukcji Zarządzania
systemem informatycznym
w Urzędzie Miasta
i Gminy w Małogoszczu

☐ Nowy użytkownik	☐ Nadanie uprawnień w systemie Informatycznym/modyfikacja	☐ Odebranie uprawnień w systemie informatycznym
Imię i nazwisko użytkownika:	Stanowisko;	

Data wystawienia:

Podpis bezpośredniego
przełożonego użytkownika
systemu:

Nadaję identyfikator:

Podpis Kierownika

Załącznik Nr 2
do „Instrukcji Zarządzania systemem informatycznym'" w Urzędzie Miasta i Gminy w Małogoszczu

W URZĘDZIE MIASTA I GMINY W MAŁOGOSZCZU EWIDENCJA UPRAWNIEŃ W ZAKRESIE DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

Lp.	Imię nazwisko użytkownika	Zakres uprawnień	Identyfikator	Data rejestracji w systemie	Data wyrejestrowania z systemu	Podpis ASI