Załącznik nr 2
do Zarządzenia Burmistrza Miasta Kościerzyna
nr 0050.196.2018
z dnia 07.12.2018 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH w Urzędzie Miasta Kościerzyna

Właściciel dokumentu

. . . . . .
Administrator Systemu Informatycznego

Zatwierdzający dokument

. . . . . .
Burmistrz Miasta Kościerzyna

Kościerzyna - 2018

I. Wstęp

Ilekroć w niniejszym dokumencie jest mowa o:

1) Urzędzie – należy przez to rozumieć Urząd Miasta Kościerzyna;
2) Instrukcji – należy przez to rozumieć niniejszy dokument;
3) Polityce Bezpieczeństwa – należy przez to rozumieć przyjęty do stosowania w Urzędzie dokument zatytułowany: „Polityka Bezpieczeństwa Informacji Urzędu Miasta Kościerzyna";
4) Użytkowniku – należy przez to rozumieć pracownika lub inną osobę działająca na rzecz Urzędu wykorzystującą system informatyczny Urzędu lub wykorzystywany przez Urząd;
5) Systemie informatycznym – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

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

1. Osoba, która ma uzyskać dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe, musi być upoważniona do przetwarzania danych osobowych (wg załącznika nr 1 do Polityki Bezpieczeństwa Informacji), oraz podpisać oświadczenie (wg załącznika nr 2 do Polityki Bezpieczeństwa Informacji).
2. Administrator Systemu Informatycznego (ASI) dokonuje nadania/odebrania osobie uprawnień w systemie informatycznym wyłącznie na podstawie pisemnego zgłoszenia takiego użytkownika. Wzór zgłoszenia użytkownika stanowi załącznik nr 1 do niniejszego dokumentu.
3. Zgłoszenia, o których mowa w pkt. 2 dokonują Kierujący Wydziałami, zastępcy Kierujących Wydziałami lub w przypadku zgłoszeń dotyczących tychże osób – ich bezpośredni przełożeni wyższego szczebla.
4. ASI przydziela danej osobie unikalny identyfikator i hasło oraz nadaje zgłoszony zakres uprawnień w systemie informatycznym.
5. ASI przekazuje osobie wskazanej w zgłoszeniu identyfikator i hasło w sposób uniemożliwiający zapoznanie się z nimi osobom trzecim.

W przypadku wygaśnięcia upoważnienia do przetwarzania danych osobowych lub odebrania uprawnień w systemie informatycznym służącym do przetwarzania danych osobowych ASI dokonuje czynności, które uniemożliwiają ponowne wykorzystanie identyfikatora użytkownika w tym systemie (jeżeli to możliwe wyłącza danego użytkownika ale nie kasuje go, jeżeli nie jest to możliwe ASI prowadzi odrębny rejestr identyfikatorów).

III. Metody i środki uwierzytelniania oraz procedury rozpoczęcia, zawieszenia i zakończenia pracy użytkowników

1. W celu uzyskania dostępu do systemu informatycznego, użytkownik podaje swój identyfikator oraz hasło.
2. Podczas opuszczenia miejsca pracy użytkownik zobowiązany jest do zablokowania dostępu do aplikacji oraz komputera poprzez zablokowanie stacji.

3. Podczas kończenia pracy użytkownik jest zobowiązany do wylogowania się, a następnie do wyłączenia komputera.
4. Komputerowe stanowiska pracy muszą być skonfigurowane w taki sposób, aby po okresie maksimum 30 minut bezczynności były one automatycznie blokowane. Do wznowienia pracy konieczne jest co najmniej ponowne użyciu hasła.
5. Hasło użytkownika w systemie informatycznym musi składać się z co najmniej 8 znaków.
6. Użytkownik, po pierwszym zalogowaniu się do systemu jest zobowiązany do zmiany hasła.
7. Zaleca się zmianę hasła co 30 dni. Jeśli system informatyczny nie wymaga dokonania takiej zmiany, każdy użytkownik jest zobowiązany do samodzielnej zmiany hasła.
8. Użytkownik jest zobowiązany do zabezpieczenia swojego hasła przed ujawnieniem osobom trzecim.
9. Do zasilania komputerowych stanowisk pracy i urządzeń peryferyjnych należy stosować tylko gniazda wydzielonej sieci elektrycznej, przeznaczone wyłącznie do zasilania sprzętu komputerowego.
10. Zakazuje się podłączania innych urządzeń (w szczególności grzejników i innego sprzętu AGD) do gniazd wydzielonej sieci elektrycznej zasilającej sprzęt komputerowy.

IV. Zasady tworzenia kopii zapasowych oraz ich przechowywania

1. Kopie zapasowe systemów kluczowych, niezbędnych do prawidłowego funkcjonowania Urzędu, wykonuje się codziennie w sposób automatyczny za pomocą przeznaczonego do tego celu oprogramowania, proces wykonywania kopii zapasowych nadzoruje na bieżąco ASI lub w sytuacjach wyjątkowych osoba go zastępująca.
2. Kopie zapasowe innych systemów i danych, które nie mogą być wykonane w sposób automatyczny wykonywane są przynajmniej raz w miesiącu. Proces wykonywania kopii zapasowych nadzoruje ASI.
3. Nośniki z kopiami zapasowymi mogą być przechowywane jedynie w pomieszczeniach o podwyższonym poziomie bezpieczeństwa fizycznego.
4. Dostęp do nośników z kopiami zapasowymi posiada ASI.
5. Możliwe jest wykonywanie zdalne kopii zapasowych w innych lokalizacjach niż główny budynek Urzędu. Wykorzystanie sieci publicznej wymaga zastosowania szyfrowanego kanału komunikacji VPN.
6. Nośniki z kopiami zapasowymi zawierającymi dane osobowe są przechowywane przez okres, w którym istnieją przesłanki do ich przetwarzania. Po ustaniu przesłanek do przetwarzania, dane muszą zostać usunięte w sposób uniemożliwiający ich odtworzenie.

V. Zabezpieczenia przed działalnością szkodliwego oprogramowania

1. Serwery i komputerowe stanowiska pracy musza być chronione przed działaniem szkodliwego oprogramowania poprzez zastosowanie systemu antywirusowego.
2. Sieć komputerowa na styku z Internetem musi być chroniona dedykowanymi do tego urządzeniami klasy firewall/UTM.
3. Do obowiązków ASI należy:
   a) zapewnienie aktualizowania systemu antywirusowego;
   b) zapewnienie aktualizowania urządzeń klasy firewall/UTM oraz utrzymanie kontroli przepływu informacji pomiędzy systemem informatycznym a Internetem.
4. ASI ma prawo stosować mechanizmy uniemożliwiające użytkownikom samodzielnie instalowanie jakiegokolwiek oprogramowania.
5. Użytkownikom nie wolno otwierać plików pochodzących z niewiadomego źródła bez zgody ASI.

VI. Wymaganie funkcjonalności systemów informatycznych

1. Dla każdej osoby, której dane są przetwarzane, system informatyczny służący do przetwarzania danych zapewnia odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu (automatycznie);
   b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu (automatycznie);
   c) źródła danych (jedynie w przypadku zbierania danych nie od osoby, której dotyczą);

2. Funkcjonalności określone w ust. 1 nie obowiązują w przypadku systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie. Dla każdej osoby, której dane osobowe są przetwarzane system informatyczny, zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust.1.

VII. Zasady dokonywania przeglądów i konserwacji

1. Okresowo ASI dokonuje przegląd systemu informatycznego, polegającego na ustaleniu poprawności działania jego elementów i funkcjonalności.
2. Regularnemu przeglądowi podlegają także nośniki z kopiami zapasowymi pod względem ich użyteczności oraz konta użytkowników systemu informatycznego w zakresie ich aktualności i prawidłowości wykorzystywania.
3. W przypadku stwierdzenia nieprawidłowości w działaniu elementów systemu informatycznego ASI podejmuje niezwłocznie czynności zmierzające do przywrócenia ich prawidłowego działania.
4. Jeżeli do przywrócenia prawidłowego działania systemu lub dokonania jego konserwacji niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności naprawcze, powinny odbywać się w obecności ASI.

VIII. Zasady użytkowania urządzeń przenośnych oraz dostępu z zewnątrz do sieci informatycznej

1. Użytkownik komputera przenośnego zawierającego dane osobowe zobowiązany jest do:
   a) zachowania szczególnej ostrożności podczas jego przenoszenia, przechowywania i użytkowania,
   b) zabezpieczenia hasłem nośników zawierających dane osobowe stosując dodatkowo środki ochrony kryptograficznej.
2. Dostęp z zewnątrz do sieci informatycznej Urzędu możliwy jest tylko w określonych przypadkach:
   a) dostęp doraźny (jednorazowy) w celu prac serwisowych z wykorzystaniem oprogramowania zaakceptowanego przez ASI i pod jego nadzorem;
   b) w uzasadnionych przypadkach dostęp stały dla wybranych pracowników Urzędu - z wykorzystaniem połączenia VPN, do którego zestawienia każdy użytkownik musi posiadać indywidualny login i hasło nadane przez ASI.
   c) w uzasadnionych przypadkach dostęp stały (na okres świadczenia usług) dla użytkowników nie będących pracownikami Urzędu, świadczących usługi na jego rzecz - z wykorzystaniem połączenia VPN, do którego zestawienia każdy użytkownik musi posiadać indywidualny login i hasło nadane przez ASI.
3. Elektroniczne nośniki pamięci, zawierające dane osobowe, przeznaczone do likwidacji uszkadza się w sposób uniemożliwiający ich odczytanie.
4. Nośniki przekazywane podmiotowi nieuprawnionemu do przetwarzania danych pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odczytanie.

Załącznik nr 1
do Instrukcji zarządzania systemem informatycznym
służącym do przetwarzania danych osobowych w Urzędzie Miasta Kościerzyna

Zgłoszenie użytkownika systemów informatycznych

Imię i nazwisko: ……

Nazwa komórki / jednostki organizacyjnej: ……

Stanowisko: ……

Proszę o nadanie/odebranie*
uprawnień w systemie informatycznym lub zmianę realizowanych funkcji - dla w/w osoby w zakresie:

Nazwa systemu / modułu	Funkcje realizowane w systemie:

Nazwa systemu / modułu	Funkcje realizowane w systemie:

Nazwa systemu / modułu	Funkcje realizowane w systemie:

Data i podpis dokonującego zgłoszenia (przełożonego):

……

- Wypełnia Administrator Systemu Informatycznego -

Nadany identyfikator w systemie informatycznym: ……..

Zmiany dokonane w zakresie funkcji realizowanych przez użytkownika w systemie oraz inne uwagi:

* niepotrzebne skreślić