Załącznik nr 2 do zarządzenia nr 11/2016

Kierownika Gminnego Ośrodka Pomocy Społecznej w Książkach

z dnia 08 grudnia 2016

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

GMINNY OŚRODEK POMOCY SPOŁECZNEJ W KSIĄŻKACH

Dokumenty powiązane:

Polityka Bezpieczeństwa Informacji

SPIS TREŚCI

§ 1

Wprowadzenie

1. Instrukcja zarządzania systemem informatycznym w Gminnym Ośrodku Pomocy Społecznej w Książkach, zwana w treści niniejszego dokumentu „Instrukcją" określa zasady postępowania jakie muszą być stosowane przez osoby przetwarzające dane osobowe w systemach informatycznych.
2. Instrukcja została opracowana w oparciu o:
   1) Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 z późn. zm.);
   2) 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.
3. Podstawowym celem zabezpieczeń systemów informatycznych jest zapewnienie jak najwyższego poziomu bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych oraz zagwarantowanie zgromadzonym danym charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności.
4. W instrukcji stosuje się następujące skróty:
   1) ADO – Administrator Danych Osobowych;
   2) ABI – Administrator Bezpieczeństwa Informacji;
   3) ASI/Informatyk – Administrator Systemu Informatycznego, odpowiedzialny za administrację systemami informatycznymi Gminnego Ośrodka Pomocy Społecznej.

§ 2

Procedura nadawania i odbierania uprawnień do przetwarzania danych osobowych

1. Przed przystąpieniem do przetwarzania danych w systemach użytkownicy zobowiązani są do zapoznania się z przepisami i zasadami przetwarzania danych osobowych.
2. Przed dopuszczeniem użytkownika do obsługi systemu powinien on odbyć szkolenie w zakresie obsługi sprzętu informatycznego, oprogramowania oraz aplikacji, która wykorzystywana będzie do realizacji zadań służbowych.
3. Pierwsze zarejestrowanie użytkownika w systemie i nadanie odpowiednich uprawnień do systemu, w którym przetwarzane są dane osobowe musi być poprzedzone złożeniem przez

użytkownika oświadczenia o zachowaniu w poufności danych osobowych i sposobu ich zabezpieczenia oraz uzyskania formalnego upoważnienia do przetwarzania danych osobowych.

4. Po spełnieniu wymagań określonych w pkt. 3 następuje nadanie uprawnień do systemów informatycznych.
5. Za nadanie uprawnień w systemie informatycznym odpowiada ASI/Informatyk. Uprawnienia nie mogą być nadane w przypadku, jeżeli dana osoba nie posiada upoważnienia do przetwarzania danych osobowych w wymaganym zakresie.
6. Identyfikator oraz zakres dostępu użytkownika powinien być rejestrowany w ewidencji osób upoważnionych do przetwarzania danych osobowych.
7. Procedurę nadania uprawnień do przetwarzania danych osobowych należy stosować odpowiednio w przypadku zmiany lub odebrania uprawnień.
8. Rozwiązanie umowy o pracę, umowy o współpracę lub utrata upoważnienia są przesłanką do natychmiastowego wyrejestrowania użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych oraz unieważnienia hasła i odnotowania tego faktu w ewidencji osób upoważnionych do przetwarzania danych osobowych.
9. Dostęp do systemu informatycznego czy do poszczególnych aplikacji i baz danych winien być możliwy tylko po podaniu identyfikatora odrębnego dla każdego użytkownika i poufnego hasła.
10. W przypadku nadania użytkownikowi uprawnień do danego systemu informatycznego po raz pierwszy, ASI/Informatyk dokonuje nadania użytkownikowi identyfikatora, wygenerowanie hasła oraz przekazuje ADO/ABI nadany osobie identyfikator w celu aktualizacji ewidencji osób upoważnionych do przetwarzania danych osobowych.
11. Hasło użytkownika jest przydzielane indywidualnie każdemu z użytkowników i znane jest tylko użytkownikowi, który się nim posługuje.
12. ASI/Informatyk przekazuje użytkownikowi identyfikator i hasło.
13. Użytkownik jest zobowiązany do zmiany hasła przy pierwszym dostępie do systemu informatycznego.
14. W przypadku konieczności odebrania lub zmiany zakresu upoważnienia, ADO niezwłocznie informuje ASI/Informatyka, który dokonuje odebrania luz zmiany zakresu uprawnień w systemie informatycznym.

§ 3

Metody i środki uwierzytelniania w systemie

1. Użytkownicy systemu informatycznego przetwarzającego dane osobowe wykorzystują w procesie uwierzytelnienia identyfikatory i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi i nie podlega zmianie.
3. Nowe hasło jest przekazywane użytkownikowi przez ASI/Informatyka.
4. Po zalogowaniu do systemu informatycznego z wykorzystaniem otrzymanego hasła użytkownik jest zobowiązany do dokonania jego natychmiastowej zmiany.
5. Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa użytkownicy systemu powinni stosować się do następujących zasad:

1) użytkownik posiada unikalny identyfikator do swojego osobistego i wyłącznego użytku;
2) hasło dostępu do systemów informatycznych powinno być utworzone przez użytkownika i stanowić tajemnicę służbową;
3) użytkownik ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie;
4) hasło nie może być ujawnione lub przekazane komukolwiek;
5) użytkownik nie powinien przechowywać hasła w widocznych miejscach.

6. Hasło dostępu do systemu informatycznego składa się z 8 znaków, zawiera litery małe i duże ora zawiera cyfry lub znaki specjalne.
1. Użytkownik zobowiązany jest do zmiany hasła nie rzadziej niż raz w miesiącu oraz w przypadku ujawnienia lub podejrzenia ujawnienia hasła.
7. W przypadku zapomnienia hasła użytkownik powinien zwrócić się do ASI/Informatyka o wygenerowanie nowego hasła.
8. Administrator Systemów Informatycznych jest odpowiedzialny za okresowe sprawdzanie systemu pod kątem występowania w nim nieaktywnych kont użytkowników.

§ 4

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Przed przystąpieniem do pracy z systemem, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest poinformować o tym fakcie bezpośrednio przełożonego. Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest zablokować swoją stacje roboczą.
3. Zawieszając pracę w systemie informatycznym, w tym odchodząc od stanowiska pracy, użytkownik blokuje stację roboczą. Kontynuacja pracy może nastąpić po odblokowaniu stacji roboczej po wprowadzeniu hasła.
4. Na stacjach roboczych stosuje się wygaszacze ekranów aktywujące się po 5 minutach od momentu braku aktywności w systemie informatycznym.
5. Opuszczając pomieszczenie, w którym przetwarzane są dane osobowe, jeżeli w pomieszczeniu tym nie przebywa inna osoba upoważniona do przetwarzania danych osobowych, pracownik zobowiązany jest do zamknięcia pomieszczenia na klucz. Zabronione jest pozostawianie bez nadzoru pomieszczeń, w których przetwarzane są dane osobowe.
6. Kończąc pracę, użytkownik obowiązany jest do wylogowania się z systemu informatycznego i zabezpieczenia stanowiska pracy, w szczególności wszelkiej dokumentacji, wydruków oraz wymiennych nośników informacji, na których znajdują się dane osobowe i umieszczenia ich w zamykanych szufladach.

§5

Wymagania w zakresie sprzętu i oprogramowania

1. Oprogramowanie musi być użytkowane z zachowaniem praw autorskich i posiadać licencję.
2. Przed instalacją nowego oprogramowania ASI/Informatyk zobowiązany jest sprawdzić jego działanie pod kątem bezpieczeństwa całego systemu.
3. Serwer winien być zasilany przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie zasilania przez co najmniej 20 minut oraz na wykonanie bezpiecznego wyłączenia serwera, tak aby przed zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na danych osobowych.
4. Pomieszczenie, w którym znajduje się serwer oraz pomieszczenia, w których przetwarzane są dane osobowe winny być odpowiednio chronione przed skutkami pożaru.
5. Należy przechowywać wszystkie poprzednie wersje oprogramowania jako środek utrzymania ciągłości działania.
6. Należy zapewnić rejestrowanie wszystkich błędów, związanych z problemami przetwarzania danych osobowych, zgłaszanych przez użytkowników lub programy systemowe.

7. Należy chronić informacje zawarte w dziennikach zdarzeń systemów przed manipulacją i nieautoryzowanym dostępem.
8. Należy zapewnić synchronizację zegarów wszystkich stosowanych systemów służących do przetwarzania danych osobowych z uzgodnionym, dokładnym źródłem czasu.

§ 6

Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Za tworzenie i przechowywanie kopii zapasowych danych znajdujących się na serwerze odpowiedzialny jest ASI/Informatyk.
2. Codzienna kopia zapasowa zapisywana jest na dysku zewnętrznym. Zapis odbywa się po godzinach pracy GOPS-u. Zapis odbywa się automatycznie.
3. Miesięczne kopie zapasowe tworzone są na dysk zewnętrzny, zapis odbywa się ręcznie.
4. Kopie zapasowe powinny być tworzone na nośnikach elektronicznych, odpowiednio opisanych, oznakowanych i ewidencjonowanych.
5. Kopie zapasowe należy opisywać w sposób umożliwiający szybką i jednoznaczną identyfikację zawartych w nich danych.
6. ASI/Informatyk odpowiedzialny za tworzenie kopii zapasowych, zobowiązany jest przestrzegać terminów sporządzania kopii zapasowych oraz okresowo dokonywać kontroli możliwości odtworzenia danych zapisanych na tych kopiach, pod kątem ewentualnej przydatności w sytuacji awarii systemu.
7. Kopie zapasowe, które uległy uszkodzeniu, powinny podlegać natychmiastowemu zniszczeniu.

§ 7

Przechowywanie nośników elektronicznych zawierających

1. Dane osobowe przechowywane są na serwerach znajdujących się w obszarach bezpiecznych, nośnikach elektronicznych oraz na stacjach roboczych znajdujących się na stanowisku pracy.
2. Po zakończeniu przetwarzania danych osobowych w postaci elektronicznej należy usunąć dane z nośnika elektronicznego w sposób uniemożliwiający ich ponowne odtworzenie.
3. Wymienne nośniki elektroniczne winny być przechowywane w zamykanych szafkach.
4. Obowiązek usunięcia danych z nośnika lub jego zniszczenie spoczywa na użytkowniku.

5. Nośniki zawierające kopie zapasowe winny być przechowywane w innym pomieszczeniu niż pomieszczenie, w którym znajduje się serwer. Dostęp do tego pomieszczenia ma ASI/Informatyk.
6. Czas przechowywania dziennych, miesięcznych kopii zapasowych określa się na rok od dnia wytworzenia.
7. Czas przechowywania rocznej kopii zapasowej określa się na dwa lata od dnia wytworzenia.
8. W przypadku wycofania sprzętu komputerowego z użycia dane osobowe na nim zapisane są kasowane przy użyciu dedykowanego oprogramowania do usuwania danych. W przypadku braku możliwości programowego usunięcia danych, dysk podlega fizycznemu zniszczeniu. Za zniszczenie danych odpowiada ASI/Informatyk. Zniszczenie nośnika potwierdzone jest protokołem.

§ 8

Ochrona przed działaniem szkodliwego oprogramowania

1. W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:

1) wprowadzanie zmian do oprogramowania, sprzętu poprzez samodzielne konfigurowanie i wyposażenie;
2) instalowania nowego oprogramowania lub aktualizacji już zainstalowanego oprogramowania;
3) korzystania z systemów informatycznych dla celów innych niż te związane z wykonywaniem zadań służbowych;
4) korzystania z prywatnego sprzętu, w tym oprogramowania oraz nośników pamięci;
5) umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych;
6) podejmowania prób testowania, modyfikowania oraz naruszania zabezpieczeń danych lub jakichkolwiek działań noszących takie znamiona;
7) kopiowania plików zawierających dane osobowe z serwerów na stacje robocze użytkowników i na nośniki informacji, chyba że zgodę na takie działania wyrazi ABI/ADO;
8) otwierając pocztę elektroniczną, nie otwierać odnośników zawartych w przesyłanych wiadomościach tzw. linków, załączniki skanować programem antywirusowym, w przypadkach wątpliwych należy skontaktować się z Informatykiem;
9) korzystania z Internetu w celach nie związanych z pełnionymi obowiązkami służbowymi.

2. W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik jest zobowiązany powiadomić ASI/Informatyka, który powiadomi ADO/ABI.
3. System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:

1) Oprogramowanie antywirusowe;
2) Zaporę sieciową;
3) Aktualizację oprogramowania systemowego;
4) Konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa.

§ 9

Przeglądy i konserwacje systemu informatycznego

1. Przeglądy, naprawy i konserwacje systemu informatycznego dokonywane są przez upoważnionych pracowników oraz podmioty zewnętrzne.
2. Prace serwisowe wykonywane na terenie Urzędu przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi ASI/Informatyka.
3. W przypadku konieczności dokonania przeglądu, naprawy lub konserwacji systemu informatycznego poza miejscem jego użytkowania z urządzenia należy wymontować element, na którym zapisane są dane osobowe, o ile jest to możliwe. W przeciwnym wypadku należy zawrzeć umowę powierzenia danych osobowych.
4. Wszelkie prace serwisowe wykonywane przez podmioty zewnętrzne wymagają sporządzenia protokołu serwisowego, zawierającego co najmniej poniższe informacje:

1) Wskazanie osoby przeprowadzającej prace serwisowe oraz podmiotu, którego osoba ta jest pracownikiem;
2) Wskazanie osoby nadzorującej przebieg prac serwisowych;
3) Przedmiot prac serwisowych, w szczególności identyfikator sprzętu;
4) Zakres prac serwisowych i ich wynik;
5) Czas przeprowadzenia prac serwisowych.

§ 10

Procedury postępowania z komputerami przenośnymi

1. Użytkownik komputera przenośnego zawierającego dane osobowe jest zobowiązany zachować szczególną ostrożność przy transporcie, przechowywaniu i użytkowaniu poza obszarem przetwarzania danych osobowych.
2. Użytkownik komputera przenośnego zawierającego dane osobowe powinien:

1) zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego – identyfikator i hasło;
2) chronić dostęp do komputera przed osobami nieupoważnionymi;
3) nie wykorzystywać komputera w obszarach użyteczności publicznej;
4) zachować szczególną ostrożność przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych;
5) transportować komputer w sposób minimalizujący ryzyko kradzieży lub zniszczenia poprzez transportowanie komputera w torbie przeznaczonej do przenoszenia komputerów przenośnych oraz nie pozostawania komputera w samochodzie itp.

3. W przypadku komputera przenośnego należy kopiować dane osobowe przetwarzane na komputerze przenośnym do systemu informatycznego w celu umożliwienia wykonania kopii awaryjnej tych danych.
4. ASI/Informatyk zobowiązany jest do podjęcia działań zmierzających do zabezpieczenia komputerów przenośnych, w szczególności aby:

1) Dokonano konfiguracji oprogramowania na komputerach przenośnych w sposób wymuszający korzystanie z haseł, jeżeli system umożliwia taką konfigurację,
2) Dokonano instalacji i konfiguracji oprogramowania antywirusowego na komputerze przenośnym.

§11

Postanowienia końcowe

W sprawach nieuregulowanych w Instrukcji mają zastosowanie przepisy Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz. U. z 2015r. poz. 2135) oraz przepisy wykonawcze do tejże Ustawy.