Ośrodek Pomocy Społecznej
ul. Kopernika 26, 72-400 Kamień Pomorski
tel./fax 913822779 / 913820279
NIP 9860029195 REGON 005464679

.....

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Zatwierdził:

KIEROWNIK
Ośrodka Pomocy Społecznej
mgr Beata Wajda 25.05.2018

.....

(data, podpis)

Niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych Ośrodka Pomocy Społecznej przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej RODO).

Definicje:

1. **Administrator Danych** – Ośrodek Pomocy Społecznej w Kamieniu Pomorskim

2. **Dane osobowe** – wszelkie informacje, w tym o stanie zdrowia, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej

3. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji, narzędzi programowych zastosowanych w celu Przetwarzania danych

4. **Użytkownik** – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych

6. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie

7. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w Systemach informatycznych

8. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym Przetwarzaniem

9. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do Przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie

10. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w Systemie informatycznym (Użytkownikowi)

I. Procedura nadawania i zmiany uprawnień

Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieupoważnione i ich ujawnienia z powodu braku świadomości konieczności ochrony danych osobowych.

1. Każdy pracownik przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
   - zasadami przetwarzania i ochrony danych osobowych zawartych w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO),
   - Polityką ochrony danych osobowych,
   - Regulaminem ochrony danych osobowych.
2. Po podpisaniu oświadczenia o zachowaniu poufności (zał. nr 1 do Instrukcji) Administrator danych osobowych lub osoba przez niego upoważniona wydaje pracownikowi Upoważnienie do przetwarzania danych osobowych (zał. nr 2 do Instrukcji) i aktualizuje wykaz osób uprawnionych do przetwarzania danych osobowych.
3. Dostęp do stacji roboczej, aplikacji, wspólnych zasobów sieciowych nadawany jest każdemu pracownikowi w formie indywidualnego identyfikatora (loginu).
4. Nadawanie, zmiana i odbieranie dostępów odbywa się na polecenie Kierownika ADO
5. Podstawę do nadania uprawnień Upoważnienie do przetwarzania danych osobowych (zał. nr 2 do Instrukcji).
6. Dostęp do elementów systemu informatycznego nadaje ADO
7. Podstawą do zmiany lub odebrania uprawnień może być udokumentowana informacja przekazana w dowolny sposób od ADO
8. Przy przydzielaniu uprawnień obowiązuje zasada minimalizacji uprawnień.
9. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielony innej osobie.
10. Użytkowników obowiązuje zasada pracy z użyciem własnego loginu. Zabroniona jest praca w jakimkolwiek elemencie systemu informatycznego na loginie innego użytkownika.

II. Polityka haseł (metody i środki uwierzytelniania)

Stosowanie polityki zapewnia, że do systemów informatycznych przetwarzających dane osobowe mają dostęp tylko osoby do tego upoważnione.
Administrator stosuje następujące wymogi w stosunku do budowy hasła, jego użytkowania i przechowywania:

1. Użytkownik komputera i aplikacji, w celu uwierzytelnienia podaje indywidualny login i hasło.
2. Hasło użytkownika powinno mieć minimum 8 znaków, zawierać co najmniej jedną dużą i jedną małą literę jedną cyfrę i znak specjalny.
3. Hasło powinno być zmieniane co miesiąc nawet, jeżeli aplikacja tego nie wymaga i nie powtarzać się częściej niż co 4 miesiące.

4. Hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitorów w formie jawnej.
5. Hasła dostępu do aplikacji, przy każdym logowaniu, powinny być wpisywane z klawiatury. Zabrania się korzystania z funkcji „Zapamiętaj mnie na tym komputerze".
6. Hasło nie powinno zawierać żadnych informacji, które można kojarzyć z użytkownikiem komputera np. osobiste dane użytkownika, tj. nazwisko, inicjały, imiona, marka lub nr rejestracyjny samochodu itp.
7. Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych.
8. Użytkownik nie może udostępnić swojego identyfikatora oraz hasła jak również dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym.
9. Hasło użytkownika należy utrzymywać w tajemnicy, również po upływie jego ważności.
10. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi systemu.
11. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów do powiadomienia o tym fakcie Administratora Danych Osobowych.
12. Aktualne hasła administracyjne do systemów, aplikacji, urządzeń przechowywane są w pokoju Kierownika, w zamykanej szafie.
13. W przypadkach awaryjnych, przy nieobecności administratora systemu, hasło może być przekazane decyzją p.o kierownika.
14. Po ustaniu sytuacji awaryjnej administrator systemu jest zobowiązany do zmiany ujawnionego hasła.
15. W przypadku utraty uprawnień przez administratora systemu należy niezwłocznie zmienić wszystkie hasła, do których miał on dostęp.

III. Procedura tworzenia kopii zapasowych

Celem procedury jest zapewnienie, że w przypadku awarii dysku, macierzy dyskowej lub zakłócenia spójności lub dostępności danych z różnych powodów istnieje możliwość ich odtworzenia.

Procedura tworzenia kopii zapasowych stanowi załącznik nr 4. Powinna ona zawierać przynajmniej informacje o:
- zawartości kopii – co zawiera np. kopia bazy danych, kopia serwera wirtualnego itp.,
- rodzaju kopii (całościowa, przyrostowa),
- nośnikach na których sporządza się kopię,
- częstotliwości sporządzania i ilości przechowywanych kopii,
- czasie i miejscu przechowywania,
- częstotliwości testowania odtwarzania kopii i osobie odpowiedzialnej za testy.

IV. Procedura niszczenia zapisów, nośników elektronicznych i dokumentów papierowych

Celem procedury jest zapewnienie, że osoby nieupoważnione nie będą miały dostępu do informacji zapisanych na nośnikach elektronicznych i w dokumentach papierowych, które utraciły swą przydatność.

1. Każdorazowo przed wycofaniem komputera z eksploatacji lub przeniesieniem na inne stanowisko należy przekazać go administratorowi systemu, by ten we właściwy sposób usunął informacje zapisane na dysku.
2. W przypadku konieczności przekazania komputera do naprawy, o ile to możliwe należy wyciągnąć z niego dysk twardy. Jeżeli nie ma takiej możliwości, to naprawa odbywa się w siedzibie Administratora danych.
3. Elektroniczne nośniki informacji (dyski twarde z komputerów i serwerów, pendrive), które nie będą już wykorzystywane z powodu uszkodzenia lub utraty możliwości ich wykorzystania składowane są w pokoju kierownika, w zamykanej szafie. Służbowe pendrive są opisane i ewidencjonowane oraz szyfrowane.
4. Okresowo wszystkie nośniki elektroniczne niszczone przez wyspecjalizowaną zewnętrzną firmę.
5. Zniszczenie nośników jest potwierdzone protokołem zniszczenia podpisanym przez osoby uczestniczące w niszczeniu.
6. Doraźnie dokumentacja papierowa niszczona jest w niszczarkach.
7. W przypadku konieczności zniszczenia dużych ilości dokumentacji papierowej jest ona przekazywana do firmy niszczącej dokumenty papierowe. Firma wystawia certyfikat potwierdzający zniszczenie dokumentów.

V. Procedura zabezpieczenia sprzętu mobilnego

Celem procedury jest wskazanie podstawowych zabezpieczeń informatycznych i fizycznych, które powinny być stosowane przy konfiguracji komputera oraz podczas jego użytkowania.

1. Administrator danych dysponuje dwoma terminalami mobilnymi, które zabezpieczone są hasłem.
2. Terminala mobilnego nie należy pozostawiać bez nadzoru w miejscach publicznych, między innymi w samochodzie.
3. Z terminala mobilnego należy korzystać w sposób minimalizujący ryzyko dostępu do przetwarzanych danych przez osoby nieupoważnione.
4. Przy korzystaniu z terminala mobilnego w miejscach publicznych i w środkach transportu publicznego należy chronić informacje wyświetlane na monitorze przed wglądem osób nieuprawnionych.
5. Zabrania się dopuszczania osób nieupoważnionych do korzystania z terminala mobilnego na którym przetwarzane są dane osobowe.
6. W przypadku kradzieży lub zagubienia terminala mobilnego należy bezzwłocznie powiadomić Administratora Danych.