Zał. nr 8 do Polityki

Regulamin ochrony danych osobowych obowiązujący w Ośrodku Pomocy Społecznej w Kamieniu Pomorskim

1. Każda osoba dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a. przetwarzania danych osobowych wyłącznie w zakresie i celu określonym w upoważnieniu do ich przetwarzania,
   b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem obowiązków służbowych,
   c. ochrony danych osobowych przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub przetwarzaniem.
2. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować.
3. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
4. Zabrania się wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia.
5. Pracownicy są zobowiązani do zabezpieczania dokumentów oraz nośników przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy np. przez zamykanie w szafach, biurkach, pomieszczeniach.
6. Zabrania się pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe po godzinach pracy.
7. Pracownicy zobowiązani są do stosowania zasady czystego biurka i czystego ekranu.

Zasady pracy w systemach informatycznych

1. Każdy pracownik zobowiązany jest do posługiwania się własnym loginem (identyfikatorem) i hasłem w celu uzyskania dostępu do systemu informatycznego.
2. Zabrania się ujawniania loginu i hasła współpracownikom i osobom z zewnątrz.
3. Zabrania się pracy w systemach informatycznych z wykorzystaniem cudzego loginu.
4. Zabrania się pracy wielu pracowników na wspólnym identyfikatorze.
5. Zabrania się uruchamiania jakichkolwiek programów na prośbę innej osoby, o ile nie została ona zweryfikowana jako uprawniona. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
6. Każdy pracownik zobowiązany jest do stosowania polityki haseł obowiązującej u Administratora, która wymaga by:
   a. hasło zawierało co najmniej 8 znaków, w tym przynajmniej jedną małą i dużą literę, cyfrę i znak specjalny,
   b. hasło było zmieniane nie rzadziej niż co 30 dni nawet gdy system tego nie wymaga,
   c. stosowane hasła były trudne do odgadnięcia,
   d. haseł nie ujawniać innym osobom,
   e. hasła przechowywać w miejscach niedostępnych dla innych osób.
7. Zabrania się wyłączania lub zmiany konfiguracji systemu antywirusowego zainstalowanego na komputerze.

Zasady korzystania z poczty elektronicznej

1. Dane osobowe przesyłane za pomocą poczty elektronicznej powinny być odpowiednio zabezpieczone (zaszyfrowane lub zabezpieczone hasłem), a hasło nie powinno być wysłane w tym samym mailu.
2. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW".
3. Użytkownicy powinni okresowo kasować maile. Dotyczy to zwłaszcza maili zawierających dane osobowe.

4. Mail służbowy jest przeznaczony do wykonywania obowiązków służbowych.
5. Zabrania się otwierania załączników (.xlsm, .exe) w mailach od nieznanych nadawców. Są to zwykle „wirusy", które mogą zainfekować komputer.
6. Zabrania się „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami".
7. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.

Zasady korzystania z internetu

1. Pracownik może korzystać z internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania programów pobranych z internetu.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie pobrane z internetu i zainstalowane na komputerze.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo.
5. Zabrania się włączania w opcjach przeglądarki internetowej zapamiętywania haseł.

Obowiązek zgłaszania podatności i incydentów zagrażających bezpieczeństwu danych osobowych

1. Każdy pracownik zobowiązany jest do powiadomienia zwierzchnika i jeżeli jest powołany IOD o podatnościach i incydentach, które mogą zagrażać bezpieczeństwu danych osobowych.
2. Do podatności, które wymagają powiadomienia, należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    b. niewłaściwe zabezpieczenie sprzętu IT i oprogramowania przed wyciekiem, kradzieżą lub utratą danych osobowych.
3. Do incydentów wymagających powiadomienia, należą:
    a. zdarzenia losowe zewnętrzne (pożar, zalanie wodą),
    b. zdarzenia losowe wewnętrzne (awarie komputerów, twardych dysków, utrata / zagubienie danych)
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych).
4. Typowe przykłady incydentów wymagające reakcji:
    a. ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
    b. niewłaściwy sposób niszczenia dokumentacji,
    c. ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
    d. ujawnienie osobom nieuprawnionym danych osobowych,
    e. telefoniczne próby wyłudzenia danych osobowych,
    f. kradzież, zagubienie komputerów lub nośników zawierających dane osobowe,
    g. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
    h. rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa informacji (pozostawienie danych w drukarce lub kserokopiarce, niewykonanie kopii zapasowych, prace na danych osobowych w celach prywatnych itp.);

Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego regulaminu są naruszeniem obowiązków pracowniczych i mogą stanowić podstawę do nałożenia kary dyscyplinarnej.