Zarządzenie nr 18/2023
DYREKTORA
Miejskiego Ośrodka Pomocy Społecznej w Zawierciu
z dnia 11 maja 2023 r.

w sprawie *wyznaczenia administratora systemów informatycznych w Miejskim Ośrodku Pomocy Społecznej w Zawierciu*

Na podstawie § 9 ust 1 Statutu Miejskiego Ośrodka Pomocy Społecznej w Zawierciu nadanego Uchwałą Nr XXXIX/357/13 Rady Miejskiej w Zawierciu z dnia 28 sierpnia 2013 r. w sprawie nadania Statutu Miejskiemu Ośrodkowi Pomocy Społecznej zmienionego treścią Uchwały Nr XVI/210/19 Rady Miejskiej w Zawierciu z dnia 30 października 2019 r. oraz Załącznika nr 6 do Polityki Ochrony Danych Osobowych w Miejskim Ośrodku Pomocy Społecznej w Zawierciu

- zarządzam -

§ 1

Wyznacza się Pana Przemysława Gawrońskiego do pełnienia funkcji administratora systemów informatycznych (ASI) w Miejskim Ośrodku Pomocy Społecznej w Zawierciu, którego zakres zadań określa Załącznik do niniejszego zarządzenia.

§ 2.

Zarządzenie wchodzi w życie z dniem 2 maja 2023 r.

Dyrektor MOPS
Martyna Tyszczak – Sołtysik

Załącznik do Zarządzenia nr 18/2023
z dnia 11 maja 2023 r. w sprawie wyznaczenia administratora systemów informatycznych
w Miejskim Ośrodku Pomocy Społecznej w Zawierciu

Zakres zadań administratora systemów informatycznych
w Miejskim Ośrodku Pomocy Społecznej w Zawierciu

I. Administrator systemów informatycznych – zwany dalej ASI, wykonuje zadania w zakresie bezpieczeństwa danych osobowych w systemie informatycznym, a w szczególności odpowiada za:
1) przeciwdziałanie dostępowi osób nieupoważnionych do systemu, w którym przetwarzane są dane osobowe oraz podejmowanie odpowiednich działań w przypadku naruszeń w systemie zabezpieczeń,
2) wdrażanie odpowiednich środków technicznych i przedsięwzięć organizacyjnych zapewniających ochronę przetwarzanych danych osobowych właściwą do zagrożeń oraz kategorii tych danych

II. ASI realizując swoje zadania współpracuje z Inspektorem Ochrony Danych oraz kierownikami komórek organizacyjnych MOPS w Zawierciu w zakresie bezpieczeństwa danych. Do czynności ASI w szczególności zalicza się:
1) współpracę przy przygotowywaniu i wdrażaniu dokumentacji ochrony danych osobowych, w szczególności instrukcji zarządzania systemem informatycznym
2) współpracę przy przeprowadzaniu okresowych planów sprawdzeń polegających na systematycznym kontrolowaniu zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności kontrolę pod kątem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem - nie rzadziej niż raz na 12 miesięcy.
3) zapewnienie ciągłości działania systemu, w tym:
a. zabezpieczenie zbiorów danych oraz programów służących do przetwarzania danych osobowych poprzez systematyczne wykonywanie kopii zapasowych
b. zabezpieczenie kopii zapasowych przed nieuprawnionym dostępem, modyfikacją, uszkodzeniem lub zniszczeniem
c. usuwanie kopii zapasowych niezwłocznie po ustaniu ich użyteczności
4) zapewnienie awaryjnego źródła zasilania oraz zabezpieczenia przed zakłóceniami w sieci zasilającej systemów informatycznych służących do przetwarzania danych osobowych, których nagła przerwa w pracy mogłaby spowodować utratę danych lub naruszenie ich integralności
5) nadzór nad naprawą oraz likwidacją urządzeń komputerowych z zachowaniem niżej wymienionych działań ochronnych:
a. urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe , uszkadza się w sposób uniemożliwiający ich odczytanie,
b. urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe przeznaczone do przekazania podmiotowi nieuprawnionemu do przetwarzania danych pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie,
c. urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe przeznaczone do naprawy pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej
6) kontrola przeglądu i konserwacji systemów informatycznych służących do przetwarzania danych osobowych, w tym m.in. wykorzystywanie jedynie oprogramowania posiadającego

wsparcie producenta oraz systematyczne, automatyczne lub zgodne z biuletynem bezpieczeństwa jego aktualizowanie, w tym również na routerach i zarządzanych przełącznikach sieciowych

7) zabezpieczenie systemów służących do przetwarzania danych osobowych przed działaniem oprogramowania złośliwego, którego celem może okazać się uzyskanie nieuprawnionego dostępu do danych poprzez zastosowanie systemu antywirusowego korzystającego z aktualnej bazy wirusów. Przy wdrażaniu tego rodzaju zabezpieczenia ASI powinien wziąć pod uwagę wszystkie systemy teleinformatyczne używane w MOPS, również te, które znajdują się na służbowych smartfonach lub tabletach
8) dostosowanie wszystkich systemów informatycznych służących do przetwarzania danych osobowych do wymogów określonych w przepisach prawa (określających warunki techniczne i organizacyjne jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych) w tym m.in. poprzez:

a. stosowanie mechanizmów kontroli dostępu do danych osobowych,
b. rejestrowanie dla każdego użytkowania odrębnego identyfikatora,
c. stosowanie haseł dostępowych składających się minimum z 8 znaków, z czego małe i duże litery, cyfry lub znaki specjalne oraz zmienianie ich nie rzadziej niż co 30 dni,
d. zapewnienie, że dostęp do systemu informatycznego jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia,
e. zapewnienie, że identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych nie może być przydzielony innej osobie ,
f. zapewnienie, że systemy odnotowują identyfikator użytkownika wprowadzającego dane osobowe do systemu (chyba, że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba),

9) zabezpieczenie pomieszczenia serwerowni przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych, w tym zabezpieczenia:

a. fizyczne (drzwi, okna itp.)
b. techniczne (elektroniczne systemy zabezpieczeń)
c. środowiskowe (zapewnienie optymalnej pracy urządzeń i ochrona przeciwpożarowa)
d. personalne
e. organizacyjne (obowiązujące w MOPS regulaminu, polityki itp.)

10) ochrona przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, w tym m.in.

a. firewalle,
b. filtry antyspamowe,
c. rozdzielenia sieci na podsieci ze względu na grupy użytkowników, usług informatycznych i systemów,
d. stosowanie filtracji MAC adresów urządzeń, które mogą uzyskać dostęp do sieci produkcyjnej,
e. odseparowanie bezprzewodowej sieci dla gości,
f. stosowanie wielu innych rozwiązań z uwzględnieniem dostępnych technologii oraz dostępnych środków finansowych

11) nadzorowanie stosowania zasady „czystego ekranu" polegającej na zakazie zapisywania przez użytkowników systemów informatycznych dokumentów zawierających dane osobowe na pulpicie komputera oraz nakazie blokowania stacji roboczej przed każdorazowym odejściem od stanowiska pracy

III. Wykonując swe czynności ASI posiada uprawnienia do:

1) Wskazywania odpowiednich zabezpieczeń technicznych i czynności organizacyjnych mających na celu zapewnienie skutecznej ochrony danych osobowych
2) Wnioskowania o pozbawieniu lub ograniczeniu zakresu przetwarzania danych osobowych i uprawnień nadanych w systemie informatycznym dla użytkowników, którzy powodują zagrożenia bezpieczeństwa i ochrony danych osobowych
3) Udzielania wytycznych dotyczących usuwania nieprawidłowości stwierdzonych w czasie

prowadzonych kontroli i dostosowywania ochrony danych do stanu zgodnego z przepisami prawa

4) Zbierania od użytkowników, ich przełożonych oraz innych osób pisemnych wyjaśnień dotyczących okoliczności powstania zagrożeń dla bezpieczeństwa i ochrony danych osobowych

Zatwierdzam

_____

/Dyrektor/