Załącznik nr 3 do Zarządzenia nr 19/2018
Dyrektora Miejskiego Ośrodka Pomocy Rodzinie w Toruniu
z dnia 16 marca 2018 w sprawie wprowadzenia w MOPR w Toruniu
Polityki Bezpieczeństwa Danych Osobowych

Instrukcja
zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Miejskim Ośrodku Pomocy Rodzinie w Toruniu

§ 1

Niniejsza instrukcja określa sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, z uwzględnieniem wymogów bezpieczeństwa informacji.

§ 2

1. W Miejskim Ośrodku Pomocy Rodzinie w Toruniu istnieją następujące zbiory danych osobowych:

1) Zbiór danych podopiecznych MOPR /pomoc społeczna/ – przetwarzany tradycyjnie i w systemach informatycznych;
2) Zbiór danych podopiecznych MOPR /rehabilitacja zawodowa/ – przetwarzany tradycyjnie;
3) Zbiór danych podopiecznych MOPR /opieka zdrowotna/ – przetwarzany tradycyjnie i w systemach informatycznych;
4) Zbiór danych podopiecznych MOPR /piecza zastępcza/ – przetwarzany tradycyjnie i w systemach informatycznych;
5) Zbiór danych o pracownikach - przetwarzany tradycyjnie i w systemach informatycznych;
6) Zbiór danych o kandydatach do pracy - przetwarzany tradycyjnie;
7) Zbiór danych o kontrahentach - przetwarzany tradycyjnie i w systemach informatycznych;
8) Zbiór danych o osobach korzystający z Zakładowego Funduszu Świadczeń Socjalnych – przetwarzany tradycyjnie;
9) Zbiór danych o oferentach - przetwarzany tradycyjnie
10) Zbiór danych klientów – skargi i wnioski – przetwarzany tradycyjnie;
11) Zbiór danych – uczestników projektów – przetwarzany tradycyjnie i w systemach informatycznych.

2. W Miejskim Ośrodku Pomocy Rodzinie w Toruniu wykorzystywane są następujące systemy informatyczne, w których przetwarza się dane osobowe:

1) System TT-Pomoc
2) e-Soda
3) Kadry
4) Kadry i Płace
5) System Bankowości Elektronicznej
6) Płatnik
7) Pożyczka
8) Księgowość budżetowa

9) System Informacji Oświatowej
10) Vulcan (biblioteka)

3. Systemy informatyczne, o których mowa w ust.2 wykorzystywane są do przetwarzania danych osobowych w poszczególnych zbiorach:

Zbiór danych	**Systemy wykorzystywane do przetwarzania danych osobowych z tego zbioru**
Zbiór danych podopiecznych MOPR /pomoc społeczna/	TT-Pomost, e-soda, System Bankowości Elektronicznej Pożyczka
Zbiór danych podopiecznych MOPR /opieka zdrowotna/	TT – Pomost Płatnik
Zbiór danych podopiecznych MOPR /piecza zastępcza/	TT-Pomost System Informacji Oświatowej System Bankowości Elektronicznej
Zbiór danych o pracownikach	Płatnik Kadry i Płace Kadry e-Soda System Bankowości Elektronicznej System Informacji Oświatowej Vulcan (biblioteka)
Zbiór danych o kontrahentach	Księgowość budżetowa e-Soda

4. Przepływ danych w ramach zbiorów odbywa się następująco:

Zbiór danych podopiecznych MOPR /pomoc społeczna/		
Program źródłowy	Program docelowy	Sposób przepływu
TT-Pomost,	System Bankowości Elektronicznej	Wymiana plików

Zbiór danych podopiecznych MOPR /opieka zdrowotna/		
Program źródłowy	Program docelowy	Sposób przepływu
TT-Pomost,	Płatnik	Wymiana plików

Zbiór danych podopiecznych MOPR /piecza zastępcza/		
Program źródłowy	Program docelowy	Sposób przepływu
TT-Pomost,	System Bankowości Elektronicznej	Wymiana plików

Zbiór danych pracowników		
Program źródłowy	Program docelowy	Sposób przepływu
Kadry i Płace	System Bankowości Elektronicznej	Wymiana plików

Kadry i Płace	Płatnik	Wymiana plików

Zbiór danych o kontrahentach nie posiada przepływu danych osobowych w formie elektronicznej.

5. Każda osoba, której dane osobowe są przetwarzane w Miejskim Ośrodku Pomocy Rodzinie ma prawo do ochrony danych osobowych jej dotyczących.
6. Za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby.
7. W Miejskim Ośrodku Pomocy Rodzinie w Toruniu, obszarem w którym przetwarzane są dane osobowe z użyciem sprzętu komputerowego, są pomieszczenia biurowe Miejskiego Ośrodka Pomocy Rodzinie w Toruniu.

§ 3

1. W obszarze przetwarzania danych, o którym mowa w § 2 ust.7 mogą przebywać wyłącznie pracownicy zatrudnieni przy przetwarzaniu danych oraz administrator bezpieczeństwa informacji, inne osoby mogą przebywać wyłącznie w obecności osób upoważnionych do przetwarzania danych osobowych.
2. Pomieszczenia w obszarze przetwarzania danych osobowych oraz te, w których przechowywane są kopie archiwalne, wydruki, elementy sieci oraz inne elementy związane z tym przetwarzaniem – muszą być na czas nieobecności pracowników zamykane na zamek patentowy uniemożliwiający dostęp do nich osób postronnych.
3. Ekrany monitorów komputerów, na których odbywa się przetwarzanie danych osobowych muszą być zlokalizowane w sposób uniemożliwiający wgląd osobom nieupoważnionym.
4. Ekrany monitorów komputerów, na których odbywa się przetwarzanie danych osobowych muszą wygaszać się automatycznie po upływie 5 minut nieaktywności użytkownika. Ponowne włączenie ekranu monitora może nastąpić po podaniu odpowiedniego hasła.
5. Po otrzymaniu informacji z zasilacza awaryjnego (sygnał dźwiękowy lub komunikat) o spadku lub zaniku napięcia w sieci energetycznej obowiązuje procedura „Zakończenia pracy”.
6. Wydruki komputerowe oraz nośniki informacji (płyty CD, DVD, dyski) zawierające dane osobowe, a przeznaczone do likwidacji winny być zniszczone w niszczarce dokumentów/ płyt.
7. Wydruki komputerowe zawierające dane osobowe, a nie przeznaczone do zniszczenia, muszą być przechowywane w szafach zamykanych na zamek uniemożliwiający dostęp do nich osób postronnych.
8. Procedura rozpoczęcia i zakończenia pracy:
   1) rozpoczęciu i zakończeniu pracy decydują użytkownicy;
   2) czynności do wykonania podczas rozpoczęcia pracy:
      a) włączyć kolejno zasilanie: zasilacz awaryjny, komputera i drukarki;
      b) jeżeli jest zainstalowane podać hasło dostępu do komputera;
      c) jeżeli jest zainstalowane podać nazwę użytkownika i hasło dostępu do systemu operacyjnego;
      d) jeżeli brak automatycznego wywoływania programu antywirusowego – uruchomić taki program;
      e) uruchomić aplikacje użytkową – podać nazwę użytkownika oraz hasło dostępu.
   3) czynności do wykonania po zakończeniu pracy:
      a) zakończyć pracę z programem użytkowanym wybierając odpowiednią funkcję lub naciskając klawisz „Esc”, wyłączyć komputer oraz zasilanie awaryjne.

9. Zabronione jest wykonywanie kopii danych osobowych oraz wydruków tych danych w celach innych niż wynikające z zasad przetwarzania danych osobowych i/lub realizacji zadań służbowych.
10. Zabronione jest wykorzystywanie systemów informatycznych do celów niezgodnych z przeznaczeniem, a w szczególności instalowanie oprogramowania innego niż niezbędne do realizacji przetwarzania danych osobowych i/lub realizacji zadań służbowych.

§ 4

1. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez Dyrektora Miejskiego Ośrodka Pomocy Rodzinie.
2. Administrator bezpieczeństwa informacji:
   1) prowadzi ewidencję (rejestry) osób upoważnionych do przetwarzania danych osobowych;
   2) na polecenie Dyrektora Miejskiego Ośrodka Pomocy Rodzinie dokonuje wyrejestrowania osoby, która utraciła uprawnienia do dostępu do danych osobowych

3. Upoważnienia wydaje się na okres obowiązywania umowy o pracę/ umowy Zlecenia/odbywania stażu.

§ 5

1. Każda osoba korzystająca z systemu informatycznego przetwarzania danych osobowych otrzymuje swój identyfikator oraz hasło dostępu. Hasła dostępu jest niejawne i znane tylko użytkownikowi.
2. Hasło dostępu jest unikalne, inne dla każdej osoby, zawiera minimum 8 znaków.
3. Hasło musi być zmieniane przynajmniej raz w miesiącu przez użytkownika.
4. Użytkownik jest zobowiązany do utrzymania hasła dostępu w tajemnicy, również po utracie jego ważności.

§ 6

1. Administrator bezpieczeństwa informacji archiwizuje bazy danych tworząc raz w miesiącu ich kopie zapasowe.
2. Kopie zapasowe:
   1) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem,
   2) usuwa się niezwłocznie po ustaniu ich użyteczności, tj. po stworzeniu nowej kopii zapasowej w następnym miesiącu.

§ 7

1. Każdy komputer musi być wyposażony w program antywirusowy, uruchamiający się automatycznie w momencie włączenia komputera.
2. Kontrola antywirusowa nośników informacji przeprowadzana jest nie rzadziej niż raz w tygodniu oraz każdorazowo przed użyciem przenośnych nośników informacji (dyskietek, płyty CD oraz DVD). Za każdym razem sprawdza się używane przenośne nośniki informacji (dyskietki, płyty CD oraz DVD).
3. Każdorazowo po pojawieniu się komunikatu o wykryciu wirusa należy niezwłocznie zawiadomić administratora bezpieczeństwa informacji.

§ 8

Przegląd i testowanie oprogramowania użytkowego i baz danych odbywa się:
1. po każdorazowej zmianie elementów oprogramowania lub struktury bazy danych;
2. po każdorazowym wgraniu bazy danych z kopii archiwalnych;
3. sprawdzanie nośników z kopiami archiwalnymi - raz w miesiącu

§ 9

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
1. likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
2. przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
3. naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§ 10

1. Konserwacje i przeglądy odbywają się przy wyłączonych komputerach tak, aby zgromadzone dane nie zostały zniszczone lub odczytane przez niepowołane osoby.
2. W przypadku konieczności oddania sprzętu do naprawy na zewnątrz, administrator bezpieczeństwa informacji ustala każdorazowo tryb postępowania (np. osobisty nadzór, demontaż dysku twardego, kasację danych, zabezpieczenie hasłem itp.).

§ 11

Nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkownika oraz kontroli dostępu do danych osobowych, w które wyposażony jest system informatyczny przetwarzający dane, sprawuje administrator bezpieczeństwa informacji.