załącznik do Zarządzenia nr 4/21
Dyrektora Miejskiego Ośrodka Sportu i Rekreacji
w Zduńskiej Woli z dnia 18 stycznia 2021r.

INSTRUKCJA BEZPIECZEŃSTWA INFORMACJI

W MIEJSKIM OŚRODKU SPORTU I REKREACJI W ZDUŃSKIEJ WOLI

Niniejsza instrukcja została opracowana w oparciu o art. 32 ust. 1 przepisów Rozporządzenia PE i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

ROZDZIAŁ 1
ZASADY WYKORZYSTYWANIA SPRZĘTU INFORMATYCZNEGO I OPROGRAMOWANIA.

1. Sprzęt informatyczny w Miejskim Ośrodku Sportu i Rekreacji w Zduńskiej Woli jest wykorzystywany jedynie do celów związanych z realizacją zadań.
2. W MOSiR wykorzystuje się następujący sprzęt informatyczny:
   a) Stacje robocze,
   b) Serwery,
   c) Komputery przenośne,
   d) Dyski zewnętrzne,
3. Jeśli wykorzystuje się stacje robocze są one wyposażone w urządzenia podtrzymujące napięcie tzw. UPS.
4. W celu realizacji zadań związanych z infrastrukturą informatyczną, Administrator korzysta z pomocy osoby obsługującej MOSiR pod względem informatycznym.
5. Administrator prowadzi ewidencję sprzętu komputerowego oraz wykaz niezbędnego oprogramowania. Prowadzenie wykazów i ewidencji może odbywać się za pomocą dedykowanych do tego narzędzi informatycznych.
6. W MOSiR wykorzystuje się jedynie legalne oprogramowanie, które posiada licencje. Za przechowywanie licencji odpowiada Administrator. Administrator zobowiązuje się do aktualizowania oprogramowania zgodnie z zaleceniami jego producentów. Administrator może zlecić obowiązek zapewnienia aktualności oprogramowania osobie obsługującej MOSiR pod względem informatycznym.
7. W MOSiR wprowadzono zasadę, że każdy użytkownik systemów komputerowych pracuje na własnym loginie i haśle. Wprowadzono zakaz udostępniania haseł innym użytkownikom oraz pracy na jednym loginie przez kilku użytkowników.

8. Użytkownicy przed dopuszczeniem do pracy w muszą odbyć szkolenie w zakresie zasad ochrony danych osobowych i użytkowania sprzętu komputerowego i oprogramowania służącego do przetwarzania danych osobowych.

9. Użytkownicy systemów informatycznych i sprzętu komputerowego otrzymują przed przystąpieniem do pracy, po spełnieniu warunku, o którym mowa w punkcie 7 niniejszego rozdziału upoważnienia z zakresem dostępu do systemów informatycznych.

10. Dopuszcza się wykorzystywanie zewnętrznych miejsc przechowywania danych (usługi w tzw. chmurze) o ile zapewniają one bezpieczeństwo i są zgodne z wytycznymi/ rekomendacjami w zakresie bezpieczeństwa.

11. Wykonuje się regularne kopie bezpieczeństwa, za których wykonanie odpowiada osoba obsługująca MOSiR pod względem informatycznym. Kopie bezpieczeństwa mogą być wykonywane z użyciem specjalistycznego, zautomatyzowanego oprogramowania. Zadaniem osoby obsługującej MOSiR pod względem informatycznym jest regularna weryfikacji poprawności ich sporządzania i możliwości ich wykorzystania. Szczegółowo zasady sporządzania kopii bezpieczeństwa reguluje Rozdział 5 niniejszego załącznika.

12. Na sprzęcie komputerowym zainstalowano wygaszacze ekranu, które po 3 minutach bez pracy ulegają automatycznemu uruchomieniu.

13. Odchodząc od stanowiska komputerowego, użytkownik winien zamknąć program służący do przetwarzania danych osobowych lub wprowadzić blokadę ekranu za pomocą klawiszy alt+ctrl+delete. Po powrocie do stanowiska pracy ponowne uruchomienie możliwości pracy powinno nastąpić po wpisaniu hasła użytkownika.

14. Zabrania się użytkownikom korzystania z internetowych sieci publicznych.

15. Zabrania się użytkownikom wykorzystywania zewnętrznych nośników danych niewiadomego pochodzenia.

16. Administrator ma obowiązek zabezpieczenia sprzętu komputerowego, systemów informatycznych, kopii bezpieczeństwa przed dostępem osób postronnych, a także przed zagrożeniami losowymi takimi jak pożar, zalanie itp.

17. Po zakończeniu pracy każdy użytkownik ma obowiązek zamknąć systemy służące do przetwarzania danych osobowych, używając opcji wylogowania się i zapisania danych przed zamknięciem systemu.

18. W przypadku korzystania z komputerów przenośnych do celów realizacji zadań służbowych w podmiocie użytkownik po zakończeniu pracy ma obowiązek zamknięcia sprzętu komputerowego w szafie zamykanej na klucz.

ROZDZIAŁ 2
DOSTĘP DO PRZETWARZANIA DANYCH OSOBOWYCH NA SPRZĘCIE KOMPUTEROWYM I SYSTEMACH INFORMATYCZNYCH

1. Dostęp do komputerów w MOSiR mają jedynie upoważnieni użytkownicy i osoba obsługująca MOSiR pod względem informatycznym, którzy posiadają indywidualne loginy i hasła dostępu.

2. Pierwsze hasło dostępowe zakłada osoba obsługująca MOSiR pod względem informatycznym na polecenie Administratora. Osoba obsługująca MOSiR pod względem informatycznym ma zakaz nadawania loginów użytkownikom, które już kiedyś wystąpiły.

3. Użytkownik, po pierwszym logowaniu, winien niezwłocznie zmienić hasło, na takie, które odpowiada postanowieniom punktu 4 niniejszego Rozdziału.

4. Hasła składają się z co najmniej 8 znaków. W skład hasła powinny wchodzić duże i małe litery, cyfra i znak specjalny. Hasło nie może być ciągiem następujących po sobie klawiszy. Zakazana jest powtarzalność hasła w okresie 12 miesięcy.

5. Użytkowników obowiązuje bezwzględny zakaz zapisywania i pozostawiania haseł w miejscach ogólnodostępnych.

6. Hasła należy zmieniać co 30 dni. Za regularność zmiany hasła odpowiada użytkownik. Administrator może zlecić osobie obsługującej MOSiR pod względem informatycznym wykorzystanie narzędzi informatycznych do wymuszania regularnych zmian hasła.

7. Postanowienia niniejszego rozdziału dotyczą również haseł dostępowych do systemów informatycznych służących do przetwarzania danych osobowych. Stosowane systemy informatyczne winny zapewniać pełną rozliczalność procesów przetwarzania danych osobowych.

8. Dopuszcza się ograniczenia w stosowaniu postanowień niniejszego rozdziału, z wyłączeniem sytuacji dotyczącej systemów informatycznych służących do przetwarzania danych osobowych, o ile na sprzęcie informatycznym nie ma zlokalizowanych żadnych plików zawierających dane osobowe, które znajdują się poza systemem informatycznym tj. dokumentów tekstowych zawierających dane osobowe, zdjęć, itp.

9. W przypadku sytuacji, o której mowa w punkcie 8 Administrator ma obowiązek zasięgnąć pisemnej opinii w tym zakresie u Inspektora Ochrony Danych Osobowych, do której dołączona jest również opinia osoby obsługującej MOSiR pod względem informatycznym o braku przeciwwskazań ze względów bezpieczeństwa.

10. Administrator wprowadził zasadę blokady dostępu do sprzętu komputerowego po trzech nieudanych próbach autoryzacji przez użytkownika. Taka sama procedura jest zalecana w przypadku dostępu do systemu informatycznego służącego do przetwarzania danych osobowych.

11. W przypadku zablokowania dostępu, użytkownik ma obowiązek powiadomić o tym fakcie osobę obsługującą MOSiR pod względem informatycznym, który przywraca mu dostęp na zasadach, o których mowa w punkcie 2-4 niniejszego rozdziału.

12. Hasło osoby obsługującej MOSiR pod względem informatycznym, którego uprawnienia są szersze niż uprawnienia użytkowników, winno składać się z co najmniej 8 znaków, w tym dużych i małych liter, cyfr i znaków specjalnych. Hasło powinno być zmieniane co najmniej raz na 30 dni, a jego powtarzalność może nastąpić dopiero po 24 miesiącach. Zakazuje się tworzenia haseł administracyjnych z wykorzystaniem imion i nazwisk czy też ciągów klawiaturowych.

ROZDZIAŁ 3
KORZYSTANIE Z INTERNETU W MIEJSKIM OŚRODU SPORTU I REKEACJI.

1. W MOSiR wykorzystuje się sieć internetową do realizacji zadań.

2. Użytkownicy wykorzystują Internet jedynie do realizacji zadań na stanowiskach pracy i do celów służbowych.

3. Użytkownicy mają bezwzględny zakaz instalowania oprogramowania niewiadomego pochodzenia. O każdorazowej potrzebie instalacji dodatkowego oprogramowania powinni powiadomić osobę obsługującą MOSiR pod względem informatycznym.

4. Użytkownicy mogą korzystać jedynie ze stron internetowych służących do realizacji zadań.

5. Wykorzystując do celów służbowych mechanizmy logowania się do zewnętrznych systemów za pomocą przeglądarek internetowych użytkownik ma bezwzględny zakaz stosowania narzędzi automatycznego zapamiętywania haseł.

6. Realizując zadania użytkownik zobowiązany jest do wykorzystywania jedynie sieci internetowej MOSiR.

7. Zabrania się pobierania plików, zgrywania plików i innych czynności narażających sieć na nieprawidłowe działanie.

ROZDZIAŁ 4
POCZTA ELEKTRONICZNA

1. Pracownicy mają prawo wykorzystywać pocztę elektroniczną do zadań na stanowiskach pracy pod warunkiem, że korzystają z adresów pocztowych MOSiR. Istnieje bezwzględny zakaz korzystania z prywatnych skrzynek do realizacji zadań pracowniczych.

2. Dopuszczalne jest wysyłanie plików zawierających dane osobowe drogą elektroniczną pod następującymi warunkami:

   a) plik zawierający dane osobowe został zaszyfrowany i jest chroniony hasłem,

   b) hasło do pliku winno spełniać kryteria, o którym mowa w punkcie 4 Rozdziału 2,

c) hasło do pliku winno być przekazane niezależnie od właściwej informacji: wiadomością sms, wiadomością telefoniczną lub w odrębnej wiadomości mailowej,

d) wiadomość mailowa powinna zawierać adnotację, że jest kierowana do konkretnego odbiorcy i powinna zawierać pouczenie, że jeśli została błędnie przesłana to jej przypadkowy odbiorca powinien ją usunąć,

e) należy zażądać potwierdzenia otrzymania wiadomości mailowej przez odbiorcę.

3. Sposoby szyfrowania plików w MOSiR określa Administrator przy udziale osoby obsługującej MOSiR pod względem informatycznym.

4. Użytkownik odbierający wiadomości mailowe ma obowiązek zachować szczególną ostrożność w przypadkach, kiedy wiadomości zawierają załączniki, w których znajdują się pliki do rozpakowania lub tzw. hiperlinki. W każdej podejrzanej sytuacji użytkownik powinien skonsultować się z osobą obsługującą MOSiR pod względem informatycznym.

5. Użytkownik ma zakaz uczestniczenia w korespondencji „zbiorowej", kiedy przesyłane są informacje z użyciem opcji „prześlij dalej" przez wielu użytkowników.

6. Wysyłając korespondencję mailową do kilku odbiorców, użytkownik ma obowiązek korzystania z opcji „UDW" tj. ukrycia odbiorców wiadomości.

7. Nie zaleca się użytkownikom przesyłania/ odbierania plików o dużych rozmiarach tj. o wielkości większej niż 5 MB.

8. Osoba obsługująca MOSiR pod względem informatycznym ma obowiązek okresowo weryfikować stan pojemności skrzynki pocztowej i w zależności od pojemności serwera i jego możliwości technicznych archiwizować zgromadzone wiadomości lub usuwać wiadomości niepotrzebne.

ROZDZIAŁ 5
WYKONYWANIE KOPII BEZPIECZEŃSTWA W MOSiR.

W celu zapewnienia ciągłości pracy oraz rozliczalności systemu ochrony danych osobowych wykonywane są kopie bezpieczeństwa baz danych.

1. Za wykonanie kopii bezpieczeństwa odpowiada osoba obsługująca MOSiR pod względem informatycznym.

2. Osoba obsługująca MOSiR pod względem informatycznym w porozumieniu z Administratorem oraz Inspektorem Ochrony Danych Osobowych określa krytyczne obszary, z których niezbędne jest sporządzanie kopii bezpieczeństwa.

3. Kopie bezpieczeństwa sporządzane są w odstępach czasowych umożliwiających zachowanie ciągłości pracy MOSiR. Częstotliwość sporządzania kopii zapasowych określa Administrator w porozumieniu z Inspektorem Ochrony Danych Osobowych.

4. Osoba obsługująca MOSiR pod względem informatycznym odpowiada za poprawność sporządzenia kopii zapasowej oraz możliwości jej wykorzystania.

5. Kopie zapasowe są nadpisywane na poprzednie jej wersje.
6. Kopia zapasowa nie może być przechowywana w pomieszczeniach, w których znajduje się podstawowa baza danych.
7. Kopie bezpieczeństwa wykonywane są w następujący sposób:
   a) Wykonuje je osobiście osoba obsługująca MOSiR pod względem informatycznym sporządzając kopię na zewnętrzny nośnik pamięci, który jest chroniony hasłem. Następnie nośnik z kopią bezpieczeństwa zostaje umieszczony w odrębnym pomieszczeniu, w szafie zamykanej na klucz*,

ROZDZIAŁ 6
ZABEZPIECZENIA TECHNICZNE I OCHRONA ANTYWIRUSOWA

1. MOSiR stosuje zabezpieczenia techniczne i ochronę antywirusową związane z systemami informatycznymi i sprzętem komputerowym.
2. W przypadku dostępu do danych osobowych za pomocą sieci zewnętrznej stosuje szyfrowanie połączeń za pomocą narzędzi typu SSL, VPN lub innych, które są powszechnie uznane za spełniające kryteria bezpieczeństwa. Zgodę na wykorzystanie takich narzędzi wydaje osoba obsługująca MOSiR pod względem informatycznym, po zasięgnięciu opinii Inspektora Ochrony Danych Osobowych.
3. W MOSiR zastosowano następujące zabezpieczenia:
   a) Blokowanie możliwości instalacji oprogramowania przez użytkownika,
   b) Blokowanie portów USB w stacjach roboczych,
   c) Budowanie topologii sieci z uwzględnieniem obszarów bezpiecznych i zdemilitaryzowanych (DMZ),
   d) Okresowe przeglądanie logów stacji roboczej przez administratorów,
4. W MOSiR, na sprzęcie komputerowym zainstalowano oprogramowanie antywirusowe, które jest na bieżąco aktualizowane.
5. Za aktualizację oprogramowania antywirusowego odpowiada osoba obsługująca MOSiR pod względem informatycznym. Zaleca się, aby oprogramowanie antywirusowe aktualizowało się automatycznie.
6. Program antywirusowy zabezpiecza co najmniej pliki systemowe oraz pocztę elektroniczną, a także ma włączoną opcję przeciwwłamaniową.
7. Użytkownik jest odpowiedzialny za skanowanie stacji roboczej/ komputera przenośnego, co najmniej raz na 3 dni.
8. Użytkownik ma bezwzględny zakaz wyłączania funkcji programu antywirusowego.

9. W przypadku podejrzenia pojawienia się szkodliwego pliku lub wirusa, użytkownik ma bezwzględny obowiązek powiadomienia o tym fakcie Administratora.

ROZDZIAŁ 7
ZASADY KORZYSTANIA Z KOMPUTERÓW PRZENOŚNYCH

1. W MOSiR dopuszcza się możliwość korzystania z komputerów przenośnych do realizacji zadań.
2. W przypadku korzystania z komputerów przenośnych użytkownicy muszą zachować szczególne środki ostrożności, które uniemożliwią kradzież sprzętu, pozostawienie go bez nadzoru.
3. Komputer przenośny, na którym przechowuje się dane osobowe musi być bezwzględnie zabezpieczony hasłem, zarówno do systemu operacyjnego, jak i do systemu informatycznego, w którym przetwarzane są dane osobowe. Hasła te nie mogą być identyczne. Zasady tworzenia haseł dostępowych są analogiczne jak w punkcie 4 Rozdziału 2 niniejszego załącznika.
4. Na komputerach przenośnych zalecane jest instalowanie dodatkowych narzędzi szyfrujących tj. specjalnych dysków i macierzy.
5. Jeśli korzystamy stacjonarnie z komputera przenośnego użytkownik ma obowiązek dbałości o jego naładowanie, które umożliwia pracę bez zasilania elektrycznego przez co najmniej 2 godziny.
6. Po zakończeniu pracy użytkownik jest zobowiązany do przeprowadzenia czynności, o których mowa w punkcie 18 Rozdziału 1 niniejszego załącznika.
7. Użytkownik ma zakaz wykorzystywania na komputerach przenośnych niezweryfikowanych sieci bezprzewodowych tj. publicznych, hotelowych i innych, które mogą umożliwić przeglądanie operacji przez osoby postronne.
8. Użytkownik jest zobowiązany do sporządzania kopii bezpieczeństwa z komputerów przenośnych w sposób uzgodniony z osobą obsługującą MOSIR pod względem informatycznym i zaakceptowany przez Administratora.

ROZDZIAŁ 8
KONSERWACJA I NAPRAWY SPRZETU INFORMATYCZNEGO I OPROGRAMOWANIA W MIEJSKIM OSRODKU SPORTU I REKREACJI.

1. Administrator przy udziale osoby obsługującej MOSiR pod względem informatycznym odpowiada za niezawodność pracy systemów informatycznych i sprzętu informatycznego, z uwzględnieniem wytycznych dostawców sprzętu i oprogramowania.
2. Konserwacja sprzętu i oprogramowania winna odbywać się w miarę potrzeb, nie rzadziej jednak niż raz do roku.

3. Administrator odpowiada za zabezpieczenie komputerów przed nieuprawnionym dostępem w trakcie napraw poza siedzibą MOSiR poprzez uprzednie, trwałe usunięcie wszystkich informacji zawierających dane osobowe. Po powrocie z naprawy, Administrator przy udziale osoby obsługującej MOSiR pod względem informatycznym, konfiguruje sprzęt w sposób umożliwiający jego powtórne wykorzystanie.
4. Naprawy i konserwacje w siedzibie MOSiR odbywać się muszą w czasie obecności lub pod nadzorem administratora lub upoważnionej przez niego osoby.
5. Administrator dopuszcza możliwość dokonywania serwisowania i napraw za pomocą narzędzi zdalnych, z zastrzeżeniem postanowień, o których mowa w punkcie 2 Rozdziału 6 niniejszego załącznika.
6. Jeśli Administrator nie ma możliwości zastosowania metod, o których mowa w niniejszym rozdziale musi zasięgnąć opinii Inspektora Ochrony Danych Osobowych o sposobach realizacji napraw i konserwacji.

ROZDZIAŁ 10
ODPOWIEDZIALNOŚĆ UŻYTKOWNIKÓW

1. Administrator jest zobowiązany do nadzoru w zakresie uprawnień użytkowników w taki sposób, aby zrealizowana została zasada minimalizacji tj. aby każdy użytkownik dopuszczony do pracy w systemach informatycznych posiadał jedynie uprawnienia niezbędne do realizacji zadań na stanowisku pracy.
2. Użytkownik odpowiada za wszystkie czynności, które zostały wykonane z użyciem jego loginu i hasła.
3. Użytkownik odpowiada również za wszystkie czynności, które doprowadziły do awarii systemów i sprzętu komputerowego w podmiocie.

Załącznik nr 1

PLAN CIĄGŁOŚCI DZIAŁANIA

Dla MOSiR przewidziano konieczność zabezpieczenia możliwości ciągłości działania dla następujących elementów:

1. z wykorzystaniem systemów informatycznych,
2. bez udziału systemów informatycznych

A. Zapewnienie ciągłości pracy systemu przetwarzania danych osobowych z udziałem systemów informatycznych

1. Wprowadza się procedurę zgłaszania awarii systemów informatycznych wykorzystywanych do przetwarzania danych osobowych w MOSiR.
2. Każdy z użytkowników systemu informatycznego, w sytuacji wystąpienia awarii tego systemu, ma obowiązek niezwłocznego zgłoszenia awarii tego systemu Administratorowi.
3. Administrator zawiadamia niezwłocznie o wystąpieniu awarii osobę obsługującą MOSiR pod względem informatycznym
4. Czas reakcji i czas naprawy określa umowa pomiędzy MOSiR a osobą wykonującą naprawy,
5. Do czasu usunięcia awarii systemu informatycznego, MOSiR wykorzystuje dokumentację papierową, która po usunięciu awarii systemu informatycznego jest niezwłocznie wprowadzana przez upoważnioną osobę do systemu.
6. Wzór dokumentacja papierowej wykorzystywanej alternatywnie w trakcie awarii systemu informatycznego nie musi być ściśle określony. Powinien jednak zawierać elementy niezbędne do kompletnego wprowadzenia danych osobowych do systemu informatycznego. Jeśli dostawca oprogramowania informatycznego przewidział taką sytuację, stosuje się szablony dokumentów papierowych dostarczonych przez dostawcę oprogramowania.
7. Po usunięciu awarii osoba obsługująca MOSiR pod względem informatycznym weryfikuje prawidłowość bazy danych, która jest uzupełniana o informacje wytworzone za pomocą zastępczej dokumentacji papierowej.
8. W przypadku uszkodzenia bazy danych należy wykorzystać kopię zapasową w celu przywrócenia poprawności systemu informatycznego.
9. Z czynności mających na celu przywrócenie pracy systemu Administrator sporządza stosowną notatkę.

B. Zapewnienie ciągłości pracy w przypadku braku dostępu do sieci internetowej

1. Jeżeli użytkownik stwierdzi brak dostępu do sieci internetowej należy to zgłosić niezwłocznie na numer pomocy technicznej dostawcy.

2. W przypadku konieczności użytkowania sieci i przedłużającej się awarii należy skorzystać z internetu mobilnego dostępnego jako alternatywne źródło.

3. Za uruchomienie łącza alternatywnego odpowiada Administrator lub wskazana przez niego osoba.

C. Zapewnienie ciągłości pracy systemu przetwarzania danych osobowych bez udziału systemów informatycznych

1. Sytuacjami, które mogą uniemożliwiać przetwarzanie danych osobowych w podmiocie bez wykorzystania systemów informatycznych mogą być:

   a) Brak możliwości dostępu do pomieszczeń, w których przetwarzane są dane osobowe,

   b) Brak możliwości wykorzystania pomieszczeń, w których przetwarzane są dane osobowe ze względu na awarię np. zalanie pomieszczenia, awaria ogrzewania.

2. W przypadku wystąpienia sytuacji, o których mowa w niniejszym rozdziale każdy z użytkowników przetwarzających dane osobowe ma obowiązek zgłoszenia tego faktu Administratorowi.

3. Administrator według najlepszej wiedzy i uznania niezwłocznie zgłasza zaistniałe usterki kompetentnym podmiotom według właściwości ich działania.

4. W przypadku braku możliwości wykorzystania pomieszczeń do przetwarzania danych osobowych z powodu awarii, Administrator jest zobowiązany wskazać użytkownikowi inne, spełniające wszystkie normy pomieszczenie na terenie MOSiR, w którym będzie on mógł kontynuować swoje obowiązki.

DYREKTOR
MIEJSKIEGO OŚRODKA SPORTU I REKREACJI
W WOLI
Małgorzata Kozak

.....
(podpis Administratora)