Załącznik Nr 3
do Zarządzenia Nr 2/2018
Dyrektora Muzeum Rybołówstwa Morskiego w Niechorzu
z dnia 26 marca 2018 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

I. Zakres stosowania

Instrukcja określa zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, a w szczególności: sposób rejestrowania i wyrejestrowania użytkownika, sposób przydziału haseł i zasady korzystania z nich, procedury rozpoczęcia i zakończenie pracy, obowiązki użytkownika, metodę i częstotliwość tworzenia kopii, zasady sprawdzania obecności wirusów komputerowych oraz dokonywania przeglądów i konserwacji systemu.

II. Obszar przetwarzania danych

1. Obszar przetwarzania danych osobowych z użyciem stacjonarnego sprzętu komputerowego w wyznaczonych pomieszczenia.
2. Wszystkie pomieszczenia, które należą do obszaru przetwarzania danych, wyposażone są w zamknięcia. W czasie, gdy nie znajdują się w nich osoby upoważnione, pomieszczenia są zamykane w sposób uniemożliwiający wstęp osobom nieupoważnionym. Osoby nieupoważnione mogą przebywać w obszarze przetwarzania danych tylko za zgodą Administratora Danych lub w obecności osób upoważnionych.

III. Rejestrowanie i wyrejestrowanie użytkownika

1. Użytkownikiem systemu informatycznego (osobą upoważnioną) może być:
   a) osoba zatrudniona przy przetwarzaniu danych osobowych w Muzeum, która posiada upoważnienie do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład,
   b) pracownik innego podmiotu lub przedsiębiorca będący osobą fizyczną prowadzi działalność na podstawie wpisu do ewidencji działalności gospodarczej, którzy świadczą na podstawie stosowanych umów usługi związane z ich pracą w systemie informatycznym (serwis, zlecenie przetwarzania danych osobowych itp.).

2. Uzyskanie uprawnień następuje na dwóch poziomach:
   a) zarejestrowania w sieci komputerowej (założenie konta),
   b) nadanie określonych uprawnień do korzystania z systemu komputerowego.

3. Pisemny wniosek o zarejestrowanie użytkownika składa bezpośredni przełożony pracownika. Wniosek zostaje przekazany do Administratora Bezpieczeństwa Informacji, który może zgłosić sprzeciw wobec przyznania uprawnień, ze względu na zagrożenie naruszenia bezpieczeństwa danych osobowych.

4. W przypadku zakończenia pracy w Muzeum, stosuje się następująca procedurę wyrejestrowania użytkownika:
   1) na karcie obiegowej, na której osoba odchodząca zbiera podpisy potwierdzenia rozliczenia się z pracodawcą, znajduje się pozycja stwierdzająca fakt usunięcia lub zablokowania profilu użytkownika,
   2) Administrator Bezpieczeństwa Informacji jako osoba upoważniona do podpisania obiegówki przed podpisaniem pozycji stwierdzającej fakt usunięcia lub zablokowania profilu użytkownika wydaje polecenie administratorowi systemu o natychmiastowym wykonaniu tej czynności,
   3) po wykonaniu tej czynności następuje podpisanie przez Administratora Bezpieczeństwa Informacji obiegówki potwierdzającej usunięcie lub zablokowanie profilu użytkownika,
   4) wykonanie tej operacji jest jednoznaczne z uniemożliwieniem dostępu do systemu dla pracownika, z którym rozwiązano umowę o pracę w Muzeum.

IV. Sposób przydziału haseł i zasady korzystania z nich

1. Każdorazowe uwierzytelnienie użytkownika w systemie następuje po podaniu loginu i hasła.
2. Używanie hasła jest obowiązkowe dla każdego użytkownika, posiadającego login w systemie.
3. W Muzeum obowiązują następujące zasady korzystania z haseł:
   a) zabrania się ujawniania haseł jakimkolwiek osobom trzecim,
   b) zabrania się zapisywania haseł lub takiego z nimi postępowania, które umożliwia lub ułatwia dostęp do haseł osobom trzecim.

4. Prawidłowe wykonywanie obowiązków związanych z korzystaniem użytkowników z haseł nadzoruje Administrator Bezpieczeństwa Informacji. Nadzór ten w szczególności polega na obserwacji (monitorowaniu) funkcjonowania mechanizmu uwierzytelniania i przywracania stanu prawidłowego w przypadku nieprawidłowości.

V. Rozpoczęcie i zakończenie pracy

1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych. W przypadku naruszenia ochrony danych osobowych użytkownik niezwłocznie powiadamia Administratora Bezpieczeństwa Informacji.
2. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:
   a) włączenia komputera,
   b) uwierzytelnienia się („zalogowania" w systemie) za pomocą loginu i hasła.
3. Niedopuszczalne jest uwierzytelnianie się na hasło i login innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika.
4. Zakończenie pracy użytkownika w systemie następuje po „wylogowaniu się" z systemu. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy,

M. Sołtek

w szczególności dyskietki, dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych.
5. W przypadku dłuższego opuszczenia stanowiska pracy, użytkownik zobowiązany jest „wylogować się" lub zaktywizować wygaszacz ekranu z opcją ponownego „logowania" się do systemu.
6. W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania („logowaniu się" w systemie), użytkownik niezwłocznie powiadamia o nich administratora.

VI. Tworzenie. Przechowywanie, sprawdzanie przydatności i likwidacji kopii zapasowych

1. Kopie zapasowe są tworzone, przechowywane i wykorzystywane z uwzględnieniem następujących zasad:
   a) kopie wykonywane są co miesiąc na płytach CD/DVD,
   b) kopie są okresowo, raz w miesiącu, sprawdzane pod kątem ich przydatności do odtworzenia danych, a jeżeli ustanie ich użyteczność są niezwłocznie usuwane.

VII. Sprawdzanie obecności wirusów komputerowych

1. Sprawdzanie obecności wirusów komputerowych dokonywane jest poprzez zainstalowanie programu, który skanuje automatycznie, bez udziału użytkownika, na obecność wirusów wszystkie pliki. Program jest zainstalowany na wszystkich stacjach roboczych.
2. Po każdej naprawie i konserwacji komputera należy dokonać sprawdzenia pod kątem występowania wirusów i ponownie zainstalować program antywirusowy.
3. Elektroniczne nośniki informacji pochodzenia zewnętrznego podlegają sprawdzeniu programem antywirusowym przed rozpoczęciem korzystania z nich. Dane uzyskiwane drogą teletransmisji należy umieszczać – przed otwarciem – w katalogu przejściowym, który podlega sprawdzeniu.

VIII. Sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków

1. Wydruki i dokumenty papierowe zawierające dane osobowe przechowywane są wyłącznie w odrębnych zamykanych szafach.
2. Osoba zatrudniona przy przetwarzaniu danych osobowych sporządzająca wydruk zawierający dane osobowe ma obowiązek na bieżąco sprawdzać przydatność wydruku w wykonywanej pracy, a w przypadku jego nieprzydatności – niezwłocznie wydruk zniszczyć.
3. Elektroniczne nośniki informacji z danymi osobowymi są oznaczane i przechowywane w zamykanych szafach lub sejfach znajdujących się w specjalnym pomieszczeniu, do którego dostęp mają wyłącznie odrębnie upoważnieni pracownicy.
4. Fizyczna likwidacja zniszczonych lub niepotrzebnych elektronicznych nośników informacji z danymi osobowymi odbywa się w sposób uniemożliwiający odczyt danych osobowych.

M. Szeel

5. Dopuszczalne jest zlecenie/powierzenie niszczenia wszelkich nośników danych osobowych wyspecjalizowanym podmiotom zewnętrznym. Podstawą przekazania danych do zniszczenia innemu podmiotowi powinna być w każdym przypadku umowa zawarta na piśmie.

IX. Zasady przeglądania i konserwacji systemu

1. Przegląd i konserwacja zbiorów danych dokonywane są poprzez:
   a) badanie spójności bazy danych,
   b) uruchamianie zapytań do bazy danych w celu analizy danych,
   c) przegląd wydruków po wyznaczonych procesach,
   d) sprawdzanie zgodności danych z dokumentami,
   e) analiza zgłaszanych uwag użytkowników.
2. Przeglądu i konserwacji dokonują specjalista ds. Informatyki w porozumieniu z Administratorem Bezpieczeństwa Informacji.
3. W przypadku zlecenia wykonywania czynności, o których mowa wyżej, podmiotowi zewnętrznemu, wszelkie prace powinny odbywać się pod nadzorem Administratora Bezpieczeństwa Informacji.

X. Komunikacja w sieci komputerowej

1. W zakresie korzystania z sieci komputerowej w Muzeum obowiązują następujące zasady:
   a) pracownicy nie są uprawnieni do instalacji jakiegokolwiek prywatnego oprogramowania. W przypadku zainstalowania takiego oprogramowania bez odpowiedniej akceptacji pracownik ponosi odpowiedzialność porządkową i prawną,
   b) oprogramowanie na komputerach może być zainstalowane wyłącznie przez informatyka,
   c) pracownicy nie mają prawa przekazywać za pośrednictwem sieci komputerowej do stron trzecich jakichkolwiek danych stanowiących własność Muzeum,
   d) pracownicy nie mogą ściągać za pośrednictwem sieci komputerowej żadnego oprogramowania,

XI. Obowiązki i odpowiedzialność użytkownika związane z obowiązywaniem Instrukcji

1. Użytkownik systemu jest zobowiązany zapoznać się z treścią niniejszej Instrukcji i potwierdzić to stosownym oświadczeniem.
2. Naruszenie przez pracownika niniejszej Instrukcji może zostać potraktowane jako naruszenie obowiązków pracowniczych i powodować określoną przepisami Kodeksu pracy odpowiedzialność pracownika.
3. Treść niniejszej Instrukcji ma charakter poufny, chroniony tajemnicą pracodawcy na zasadzie art. 100 § 2 pkt. 4 Kodeksu pracy.