Załącznik Nr 2
do zarządzenia nr 6/2013
z dnia 18.12.2013r.

Instrukcja zarządzania systemem informatycznym w Gminnej Bibliotece Publicznej w Baruchowie

§ 1
Postanowienia ogólne

1. Instrukcję niniejszą opracował administrator danych osobowych w Gminnej Bibliotece Publicznej w Baruchowie na podstawie Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.), Rozporządzenia Ministra Spraw Wewnętrznych z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r., Nr 100, poz. 1024).
2. Celem wprowadzenia instrukcji jest wskazanie ramowych zasad właściwego zarządzania zabezpieczeniami systemu informatycznego oraz ochrony danych osobowych przetwarzanych w tym systemie.
3. Podstawowym obowiązkiem administratora danych, przed przystąpieniem do przetwarzania danych osobowych, jest:

a) określenie celu, strategii i polityki zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe;
b) przeanalizowanie i zidentyfikowanie zagrożenia i ryzyka, na które może być narażone przetwarzanie danych osobowych;
c) określenie potrzeb w zakresie zabezpieczenia zbiorów danych osobowych i systemów informatycznych, z uwzględnieniem potrzeby kryptograficznej ochrony danych osobowych, w szczególności podczas ich przesyłania za pomocą urządzeń teletransmisji danych;
d) określenie zabezpieczeń adekwatnych do zagrożeń i ryzyka;
e) monitorowanie działania zabezpieczeń wdrożonych w celu ochrony danych osobowych i ich przetwarzania;
f) opracowanie i wdrożenie programów szkoleń w zakresie zabezpieczeń systemu informatycznego;
g) wykrywanie i właściwe reagowanie na przypadki naruszenia bezpieczeństwa danych osobowych i systemów informatycznych je przetwarzających.

4. Administrator danych osobowych jest odpowiedzialny za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie.
5. Niniejsza instrukcja zawiera w szczególności:

a) określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmiany;
b) określenie sposobu rejestrowania i wyrejestrowywania użytkowników;
c) procedury rozpoczęcia i zakończenia pracy;
d) metodę i częstotliwość tworzenia kopii awaryjnych;
e) metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz sposób ich usuwania;
f) sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków;
g) sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych, sposób postępowania w zakresie komunikacji w sieci komputerowej.

§ 2
Procedury nadawania uprawnień do przetwarzania danych i rejestracja tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Każda osoba upoważniona do pracy w systemie informatycznym, w którym przetwarzane są dane osobowe (użytkownik systemu), winna posiadać własny identyfikator i hasło dostępu.
2. O przyznaniu identyfikatora decydować będzie administrator danych osobowych.
3. Każdy z użytkowników przed dopuszczeniem do systemu podpisze oświadczenie o zachowaniu poufności, zapozna się z niniejszą „Instrukcją" i „Polityką bezpieczeństwa" oraz zostanie pouczony o wdrożonych procedurach bezpieczeństwa.
4. Administratorowi przysługuje prawo do zablokowania konta użytkownika w każdym czasie.
5. Identyfikator wraz z danymi użytkownika podlega wpisowi od ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych oraz rejestracji w systemie informatycznym.
6. Dostęp do danych osobowych przetwarzanych w systemie informatycznym możliwy jest wyłącznie po podaniu przez użytkownika identyfikatora i hasła dostępu.
7. W przypadku awarii, zagubienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu danych każdy z użytkowników obowiązany jest niezwłocznie powiadomić administratora danych osobowych.
8. Identyfikator użytkownika nie podlega zmianom ani przydziałowi innym użytkownikom.
9. W przypadku utraty przez użytkownika uprawnień do dostępu do danych osobowych należy niezwłocznie dokonać stosownej adnotacji w ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych, wyrejestrować identyfikator z systemu informatycznego, w którym przetwarzane są dane (ewentualnie anulować uprawnienie dostępu do bazy danych), unieważnić jego hasło oraz podjąć inne niezbędne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

§ 3
Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Użytkownicy zostaną powiadomieni o pierwotnym haśle dostępu do systemu pisemnie ze stosownym pouczeniem o poufnym charakterze hasła oraz obowiązku zachowania go w tajemnicy i zakazie ujawniania go osobom trzecim, w tym innym użytkownikom.
2. Każdy z użytkowników odbędzie szkolenie dotyczące zasad bezpieczeństwa, procedur postępowania w przypadku zagubienia hasła oraz postępowania w sytuacjach awaryjnych.
3. Użytkownik obowiązany będzie zapamiętać hasło, o którym mowa powyżej.
4. W momencie pierwszego logowania w systemie przy użyciu tymczasowego hasła pierwotnego system wymusi na użytkowniku dokonanie niezwłocznej zmiany hasła tymczasowego (pierwotnego) na inne hasło spełniające kryteria opisane w niniejszej „Instrukcji".
5. Hasło składać się będzie z ciągu co najmniej 8 znaków (małe i wielkie litery oraz cyfry lub znaki specjalne).
6. Hasła będą różne dla każdego z użytkowników.
7. Hasła będą przechowywane w systemie w postaci zaszyfrowanej.
8. Login i hasło przyznane jednemu z użytkowników nie może zostać powtórnie wykorzystane.
9. Hasła będą zmieniane nie rzadziej niż co 30 dni.
10. Osobą odpowiedzialną za przydzielenie haseł będzie administrator danych osobowych.

§ 4

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkownika systemu

1. Użytkownik przystępujący do pracy w systemie informatycznym, w którym przetwarzane są dane osobowe, wpisuje identyfikator oraz hasło dostępu, a po uzyskaniu akceptacji uruchamia właściwą aplikację.
2. Użytkownik podczas logowania do systemu nie może ujawnić hasła osobom trzecim, w tym innym użytkownikom, oraz pozostawić zapisanego hasła w pobliżu systemu i innych pracowników.
3. Krótkotrwałe przerwy w pracy (bez opuszczania stanowiska pracy) nie wymagają zamykania aplikacji.
4. Przed opuszczeniem stanowiska pracy użytkownik zobowiązany jest do wylogowania się z systemu.
5. Wylogowanie następuje poprzez wybranie w systemie opcji „wyloguj" lub zablokowanie ekranu w sposób, który uniemożliwia odblokowanie go bez znajomości hasła.
6. Po zakończeniu pracy należy zamknąć aplikację i po zastosowaniu odpowiedniej procedury wyłączyć komputer.
7. Osoby użytkujące przenośny komputer, służący do przetwarzania danych osobowych, obowiązane są zabezpieczyć dostęp do komputera hasłem, zachować szczególną ostrożność podczas transportu i przechowywania komputera, nie zezwalając na używanie komputera przez osoby nieupoważnione.

§ 5

Procedury tworzenia kopii zapasowych zbiorów danych

Kopie bazy danych zapisywane są automatycznie na serwerze centralnym programu MAK+

§ 6

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopi zapasowych

1. Nośniki informacji oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępnienia, przechowuje się w wydzielonym pomieszczeniu, w warunkach uniemożliwiających ich uszkodzenie lub zniszczenie oraz dostęp osobom niepowołanym.
2. Czas przechowywania ustala administrator danych osobowych, zależnie od rodzaju danych, w oparciu o ocenę ich przydatności i obowiązujące przepisy prawa.
3. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, należy wcześniej pozbawić zapisu danych, a gdy nie jest to możliwe, uszkodzić w sposób uniemożliwiający ich odczytanie.
4. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, należy uprzednio pozbawić zapisu tych danych.
5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, należy pozbawić przed naprawą zapisu danych albo naprawić pod nadzorem osoby upoważnionej przez administratora danych.
6. Wydruki zawierające dane osobowe, przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 7

Sprawdzanie obecności wirusów komputerowych

1. System chroniony będzie przed działaniem wirusów komputerowych oprogramowaniem antywirusowym aktualizowanym na bieżąco.

2. W celu przeciwdziałania atakom zainfekowanych plików system będzie skanowany przez administratora danych osobowych co 24 godziny pod kątem obecności w systemie wirusów i innych zagrożeń.
3. Bez zgody administratora danych osobowych zabronione jest instalowanie jakiegokolwiek oprogramowania komputerowego.
4. Pobieranie w niezbędnym zakresie danych ze źródeł zewnętrznych możliwe jest wyłącznie po uprzednim ich sprawdzeniu pod kątem obecności wirusów komputerowych.

§ 8
Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia

1. System informatyczny zapewnia odnotowanie informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.
2. Odnotowanie następuje przez automatyczny zapisek w systemie okoliczności, o której mowa powyżej.

§ 9
Przegląd i konserwacja systemu i zbioru danych osobowych

Administrator danych osobowych raz na miesiąc, a w przypadku podejrzeń naruszenia zabezpieczeń danych osobowych z uwagi na stan urządzeń lub sposób działania programu bezzwłocznie:

a) dokonuje sprawdzenia serwera oraz poszczególnych komputerów za pomocą istniejących w systemie informatycznym programów monitorujących,
b) dokonuje przeglądu i bieżącej konserwacji sprzętu oraz zbioru danych.

§ 10
Postanowienia końcowe

1. Administrator danych prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych.
2. Osoba wpisana do ewidencji zobowiązana jest do odbycia stosownego przeszkolenia w zakresie ochrony danych, zapoznania się z treścią Ustawy o ochronie danych osobowych oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, a także „Polityką bezpieczeństwa" i obowiązującymi instrukcjami. Wykonanie powyższych zobowiązań pracownik potwierdza własnoręcznym podpisem.
3. Wszelkie zmiany powyższej instrukcji skutkują wobec osób, których dotyczą, z dniem ich doręczenia na piśmie.
4. Instrukcja wchodzi w życie z dniem podpisania.

KIEROWNIK
Gminnej Biblioteki Publicznej
w BARUCHOWIE
Danuta Albińska