Załącznik do zarządzenia nr 2 KZ/ 2017 z dnia 23 lutego 2017 roku

Instrukcja

zarządzania systemem przetwarzania danych osobowych

przy użyciu systemu informatycznego
i w sposób tradycyjny
w Szkole Muzycznej I stopnia
w Dobczycach

Opracował:
Dyrektor Szkoły
Muzycznej I stopnia
w Dobczycach
mgr Monika Gubała

Spis treści

Podstawa prawna:

- Art. 36 *ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (tekst jedn.: DzU 2002 nr 101, poz. 926 ze zm.).

- § 3 i § 4 *Rozporządzenia Ministra Spraw Wewnętrznych i Administracji 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* (DzU 2004 nr 100, poz. 1024).

1. Nadawanie uprawnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym

1. Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych, wydane przez Administratora Danych Osobowych.
2. Upoważnienia do przetwarzania danych osobowych, o których mowa w punkcie 1 przechowywane są w teczkach akt osobowych pracowników oraz prowadzona jest ich ewidencja.
3. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po:
   - podaniu identyfikatora użytkownika i właściwego hasła w przypadku obsługi programów SIO
   - podaniu właściwego hasła dostępu do stanowiska komputerowego w przypadku obsługi programów Office, Windows.
4. Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, Administrator Bezpieczeństwa Informacji ustala niepowtarzalny identyfikator i hasło początkowe.
5. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
6. W przypadku utraty przez daną osobę uprawnień do dostępu do danych osobowych w systemie informatycznym, identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić jej hasło oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych. Za realizację procedury rejestrowania i wyrejestrowywanie użytkowników w systemie informatycznym odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

2. Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Dane osobowe przetwarzane są z użyciem dedykowanych serwerów, komputerów stacjonarnych.
2. Hasło użytkownika powinno mieć minimum 8 znaków i być zmieniane w przypadku stanowiska komputerowego co 40 dni.
3. Hasło oprócz znaków małych i dużych liter winno zawierać znaki alfanumeryczne i specjalne.
4. Hasło powinno być tak zbudowane, aby nie można było go kojarzyć z użytkownikiem komputera – przykładowo dane osobiste: nazwisko, inicjały, imiona, data urodzin własna, dziecka lub małżonka, imię domowego zwierzaka itp.
5. Hasło użytkownika, umożliwiające dostęp do systemu informatycznego, należy utrzymywać w tajemnicy, również po upływie jego ważności.
6. Hasło nie może znajdować się w miejscu widocznym oraz nie mogą mieć do niego dostęp osoby nieuprawnione. Użytkownikowi nie wolno udostępnić swojego loginu i hasła, jak również dopuszczać osoby nieuprawnione do stanowiska roboczego po uwierzytelnieniu w systemie.
7. Raz przypisany login nie może być przydzielony innemu użytkownikowi lub po przerwie (przerwa w zatrudnieniu) w pracy temu samemu pracownikowi.
8. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła.

9. Nowo przyjęty pracownik po przydzieleniu loginu i „hasła jednorazowego” zobowiązany jest do jego zmienienia przy pierwszym logowaniu się do systemu.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy

1. Dane osobowe, których administratorem jest Szkoła Muzyczna I stopnia w Dobczycach, mogą być przetwarzane sposobem tradycyjnym lub z użyciem systemu informatycznego tylko na potrzeby realizowania zadań statutowych i organizacyjnych szkoły.
2. Rozpoczęcie pracy użytkownika w systemie informatycznym następuje po poprawnym uwierzytelnieniu (zalogowaniu się do systemu).
3. Rozpoczęcie pracy w aplikacji musi być przeprowadzone zgodnie z instrukcją zawartą w dokumentacji aplikacji.
4. Zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się z systemu oraz poprzez uruchomienie odpowiedniej dla danego systemu opcji jego zamknięcia, zgodnie z instrukcją zawartą w dokumentacji.
5. Niedopuszczalne jest zakończenie pracy w systemie bez wykonania wylogowania się z aplikacji i zamknięcia systemu.
6. Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, w których przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, a na których przetwarzane są dane osobowe, należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w monitor komputera.
7. Użytkownik ma obowiązek wylogowania się w przypadku zakończenia pracy. Stanowisko komputerowe nie może pozostać z włączonym i dostępnym systemem bez nadzoru pracującego na nim pracownika.
8. Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym do nich dostęp osobom postronnym. Wydruki niepotrzebne należy zniszczyć w niszczarce dokumentów.
9. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.
10. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać, na czas nieobecności osób zatrudnionych, w sposób uniemożliwiający dostęp do nich osobom trzecim.
11. Użytkownik niezwłocznie powiadamia Administratora Bezpieczeństwa Informacji w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane narzędzia programowe lub sprzętowe. Wówczas, użytkownik jest zobowiązany do natychmiastowego wyłączenia sprzętu.

4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania

1. Zbiory danych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
   - urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
   - sporządzania kopii zapasowych zbiorów danych (kopie pełne).
2. Za tworzenie kopii bezpieczeństwa systemu informatycznego odpowiedzialny jest Administrator Bezpieczeństwa Informacji.
3. Pełne kopie zapasowe zbiorów danych są tworzone co najmniej raz w miesiącu.
4. W przypadku aktualizacji lub dokonywania zmian w systemie należy obowiązkowo wykonać kopię zapasową systemu.
5. W przypadku awarii systemu kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia. Za przeprowadzanie tej procedury odpowiedzialny jest Administrator Bezpieczeństwa Informacji.
6. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.

5. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

1. Okresowe kopie zapasowe wykonywane są na dysku zewnętrznym lub innych elektronicznych nośnikach informacji. Kopie zapasowe przechowuje się w kasie pancernej w pomieszczeniu dyrektora szkoły, w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
2. Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych osobowych ma wyłącznie Administrator Bezpieczeństwa Informacji.
3. Wszelkimi sprawami kopi księgowości zajmuje się Centrum Usług Wspólnych ul. Rynek 21, 32410 Dobczyce przy Urzędzie Gminy i Miasta Dobczyce.
4. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji.
5. W przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika – odpowiedzialny za ich zniszczenie jest użytkownik.
6. Przez zniszczenie nośników informacji rozumie się ich trwałe i nieodwracalne zniszczenie do stanu niedającego możliwości ich rekonstrukcji i odzyskania danych.

6. Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. W związku z istnieniem zagrożenia dla zbiorów danych osobowych ze strony złośliwego oprogramowania, którego celem jest m.in. uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych.
2. Wirusy komputerowe mogą rozpowszechniać się w systemach szkoły poprzez: Internet, nośniki informacji takie jak: płyty CD i DVD, przenośne dyski, pendrive itp.
3. Przeciwdziałanie zagrożeniom ze strony złośliwego oprogramowania realizowane jest następująco:
    1) Komputer z dostępem do Internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego i firewall (zapora).
    2) Zainstalowany program antywirusowy powinien być tak skonfigurowany, by co najmniej raz dziennie dokonywał aktualizacji bazy wirusów oraz co najmniej raz w tygodniu dokonywane było automatycznie sprawdzenie komputera pod kątem obecności wirusów komputerowych.
    3) Elektroniczne nośniki informacji takie jak dyskietki, dyski przenośne, należy każdorazowo sprawdzać programem antywirusowym przed użyciem, po zainstalowaniu ich w systemie. Czynność powyższą realizuje użytkownik systemu. W przypadku problemów ze sprawdzeniem zewnętrznego nośnika danych użytkownik jest zobowiązany zwrócić się z tym do Administratora Bezpieczeństwa Informacji.
    4) Komputery i systemy muszą mieć zainstalowany program antywirusowy, a w przypadku komputerów z dostępem do Internetu, również posiadać oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem z sieci (firewall).
4. W przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego wskazujący na zaistnienie zagrożenia lub rozpoznanie tego typu zagrożenie, zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z Administratorem Bezpieczeństwa Informacji.
5. Przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. Zabrania się otwierania załączników i wiadomości poczty elektronicznej od nieznanych nadawców.
6. Zabrania się użytkownikom komputerów wyłączania, blokowania, odinstalowywania programów zabezpieczających komputer (skaner antywirusowy, firewall) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.
7. Zabrania się ściągania się na komputery i nośniki danych oprogramowania z Internetu.
8. Zabrania się nieautoryzowanego instalowania własnego oprogramowania na służbowych komputerach.

6. Udostępnianie danych osobowych i sposób odnotowania informacji o udostępnionych danych

Udostępnienie danych instytucjom może odbywać się wyłącznie zgodnie z przepisami prawa (np.: CEA, Urząd Gminy i inne).

7. Wykonywanie przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych

1. Przeglądy i konserwacje systemu oraz zbiorów danych wykonuje na bieżąco Administrator Bezpieczeństwa Informacji.
2. Administrator Bezpieczeństwa Informacji okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej.
3. Umowy dotyczące instalacji i konserwacji sprzętu należy zawierać z podmiotami, które gwarantują wykonanie prawidłowo usług.
4. Naprawy sprzętu należy zlecać podmiotom, które gwarantują wykonanie prawidłowo usług. Naprawa sprzętu, na którym mogą znajdować się dane osobowe, powinna odbywać się pod nadzorem Administratora Bezpieczeństwa Informacji w miejscu jego użytkowania.
5. W przypadku konieczności naprawy w serwisie, sprzęt komputerowy przed oddaniem do serwisu powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośniki informacji, a dyski twarde, bezwzględnie wymontować na czas naprawy lub trwale usunąć z nich dane.
6. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji może być dokonana tylko za wiedzą i zgodą Administratora Bezpieczeństwa Informacji.

8. Ustalenia końcowe

1. Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe w szkole zabrania się:
   - ujawniania loginu i hasła współpracownikom i osobom z zewnątrz,
   - pozostawiania haseł w miejscach widocznych dla innych osób,
   - udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,
   - udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie,
   - używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,
   - przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne,
   - kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza szkołę,
   - samowolnego instalowania i używania jakichkolwiek programów komputerowych, w tym również programów do użytku prywatnego; programy komputerowe instalowane są przez Administratora Bezpieczeństwa Informacji,
   - używania nośników danych udostępnionych przez osoby postronne,
   - przesyłania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego,
   - otwierania załączników i wiadomości poczty elektronicznej od nieznanych i nieznanych nadawców,
   - używania nośników danych prywatnych, niesprawdzonych, niewiadomego pochodzenia. W sytuacji, gdy zaistniała konieczności użycia niesprawdzonych przenośnych nośników danych, należy przeskanować je programem antywirusowymi, a w razie jakiś ostrzeżeń wyświetlonych przez program antywirusowy, zgłosić to Administratorowi Bezpieczeństwa Informacji.

2. Użytkownikowi nie wolno:

- wyrzucać dokumentów zawierających dane osobowe (dokumenty zawierające dane osobowe mogą być niszczone tylko w niszczarce),
- pozostawiać dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach,
- pozostawiać kluczy w drzwiach, szafach, biurkach, pozostawiać otwartych pomieszczeń, w których przetwarza się dane osobowe,
- pozostawiać bez nadzoru osoby trzecie przebywające w pomieszczeniach szkoły, w których przetwarzane są dane osobowe,
- pozostawiać dokumentów na biurku po zakończonej pracy, pozostawiać otwartych dokumentów na ekranie monitora bez blokady konsoli,
- ignorować nieznanych osób z zewnątrz, poruszających się w obszarze przetwarzania danych osobowych,
- przekazywać informacji będącymi danymi osobowymi osobom nieupoważnionym.

3. **Użytkownik zobowiązany jest do:**
   - posługiwania się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych,
- tworzenia haseł trudnych do odgadnięcia dla innych,
- używanie konta służbowego tylko w celach służbowych,
- niezakańczania procesu skanowania przez program antywirusowy na komputerze,
- wykonywania kopii zapasowych danych przetwarzanych na stanowisku komputerowym (pliki MS Office),
- zabezpieczenia sprzętu komputerowego przenośnego (laptopy) przed kradzieżą lub nieuprawnionym dostępem do danych.

4. Wszelkie przypadki naruszenia niniejszej Instrukcji należy zgłaszać Administratorowi Bezpieczeństwa Informacji lub bezpośredniemu przełożonemu.

5. Dane kontaktowe

   Administrator Bezpieczeństwa Informacji – sekretariat szkoły , nr tel.:12 274-20-78, email: szkolamuzyczna@dobczyce.pl

9. Zalecenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym

1. Miejscem tworzenia, uzupełniania i przechowywania dokumentacji dotyczącej przetwarzania danych osobowych sposobem tradycyjnym, są pomieszczenia w szkole: sekretariat, pokój nauczycielski, gabinet dyrektora, biblioteka.
2. Osoby prowadzące dokumentację zobowiązane są do zachowania tajemnicy służbowej.
3. Dokumentacji, o której mowa w punkcie 10.1. nie można wynosić poza teren szkoły.
4. Dokumentację, o której mowa w punkcie 10.1. archiwizuje się zgodnie z Instrukcją kancelaryjną.
5. Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania dyrektora o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.

Regulamin wchodzi w życie z dniem 23 lutego 2017 r.