INSTRUKCJA

ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

Szkoły Podstawowej nr 1 w Bytowie,
ul. Mierosławskiego 7, 77-100 Bytów

Data wprowadzenia:	
Wersja:	**1**
Data utworzenia:	**05.03.2026 r.**
Opracował:	**Piotr Przyborowski (IOD)**
Zatwierdził:	

SPIS TREŚCI

1. Wprowadzenie

Instrukcja została opracowana zgodnie z wymogami §5 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 (Dz. U. Nr 100, poz. 1024).

Niniejsza instrukcja stanowi zestaw procedur opisujących zasady bezpieczeństwa danych osobowych przetwarzanych w zbiorach papierowych oraz w systemach informatycznych Szkoły Podstawowej nr 1 w Bytowie.

2. Zakres stosowania Instrukcji Zarządzania Systemami Informatycznymi

Procedury i zasady określone w niniejszym dokumencie powinny być znane i stosowane przez wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych Szkoły Podstawowej nr 1 w Bytowie, bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy.

3. Procedura nadawania uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym

1) W celu zapewnienia wyłącznie prawidłowego i uzasadnionego dostępu do systemu informatycznego oraz dla zapobiegania nieuprawnionemu dostępowi do systemu informatycznego, nadawanie uprawnień do systemów teleinformatycznych odbywa się z uwzględnieniem poniższych zasad:

a) Pracownikowi mogą być nadane uprawnienia, które są konieczne do realizacji zleconych mu zadań.

b) Uprawnienia do systemu nadawane są przez Administratora Systemów Informatycznych lub Administratora Danych Osobowych.

c) Pracownikom nadawane są unikalne identyfikatory. Nazwy kont pracowników muszą zapewniać jednoznaczną identyfikację.

d) Konta umożliwiające działania administracyjne (np. Administrator) muszą zapewniać pełną rozliczalność i identyfikalność działań. W tym celu konta z uprawnieniami administracyjnymi winny być przypisane do konkretnych osób.

e) Hasła administracyjne ustala Administrator Systemów Informatycznych lub Administrator Danych Osobowych.

f) Administratora Systemów Informatycznych jest zobowiązany do prowadzenia metryk haseł administratora i przechowywania ich w zabezpieczonych miejscach, do których dostęp ma także Administrator Danych Osobowych.

g) Wszyscy użytkownicy systemu zobowiązani są do stosowania polityki haseł zgodnie z wytycznymi zawartymi w punkcie 4 poniższej Instrukcji.

h) Wszelkie zmiany dotyczące użytkownika, takie jak rozwiązanie umowy o pracę lub cofnięcie upoważnienia do przetwarzania danych osobowych są przesłanką do niezwłocznego zablokowania konta użytkownika systemu informatycznego.

4. Stosowane metody i środki uwierzytelniania oraz procedury związanych z ich zarządzaniem i użytkowaniem

1) Wymagania odnośnie tworzenia i używania haseł i identyfikatorów:

a) Hasło musi zawierać nie mniej niż 8 znaków.
b) Hasło musi składać się z liter (małych i dużych) oraz cyfr i znaków specjalnych.
c) Hasła nie mogą być ujawniane innym nieupoważnionym osobom.
d) Hasła do różnych systemów powinny być różne, za wyjątkiem sytuacji, gdy jest możliwe zastosowanie mechanizmu jednokrotnego logowania.
e) Hasła nie mogą być przechowywane w czytelnej postaci (zarówno jako tekst w pliku jak i zapisane na papierze) w sposób umożliwiający ich przejęcie. Wyjątkiem jest zdeponowanie haseł użytkowników, jak i administratorów w bezpiecznym miejscu (sejfie, szafie pancernej lub w równoważnym miejscu).
f) Hasło powinno zostać niezwłocznie zmienione w przypadku ujawnienia lub podejrzenia ujawnienia osobie nieuprawnionej.
g) Hasła tymczasowe lub startowe powinny być zmienione po pierwszym logowaniu.
h) Hasła domyślne tzw. defaultowe powinny być niezwłocznie zmienione.
i) W przypadku zakończenia świadczenia pracy lub odbiorze upoważnienia do przetwarzania danych, konto użytkownika powinno zostać niezwłocznie zablokowane.
j) Identyfikator raz użyty nie może być wykorzystywany ponownie.
k) Hasła powinny być trudne do odgadnięcia (zaleca się nie stosować nazw potocznych, imion, nazwisk, dat urodzenia, numerów dokumentów, innych danych osobistych oraz standardowych kombinacji znaków, np. 12345678).
m) Powinna zostać tworzona historia haseł w celu zablokowania ich powtarzania.

5. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym

1) Stosowane są następujące zasady rozpoczęcia pracy w systemie informatycznym:

a) Przed przystąpieniem do pracy, użytkownik zobowiązany jest do sprawdzenia czy stacja robocza wykorzystywana do przetwarzania danych osobowych w systemie informatycznym nie wskazuje na ingerencję osób trzecich, a także czy stanowisko pracy zastano w takim stanie jak pozostawiono po zakończeniu pracy.

b) Przed uruchomieniem stacji roboczej, użytkownik zobowiązany jest do upewnienia się, czy ekran monitora jest ustawiony w sposób uniemożliwiający osobom nieupoważnionym podglądnięcie jego zawartości.

c) Każde rozpoczęcie pracy w danym systemie wymaga logowania.

d) W trakcie pracy, użytkownik powinien mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych.

e) W trakcie pracy, użytkownik powinien mieć na biurku tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych.

2) Stosowane są następujące zasady zawieszenia pracy w systemie informatycznym:

a) W przypadku chwilowego opuszczenia stanowiska pracy użytkownik zobowiązany jest do wylogowania się z systemu bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji przez osoby niepowołane.

b) W przypadku opuszczenia stanowiska pracy materiały zawierające dane wymagające ochrony powinny być zabezpieczane przed dostępem osób nieuprawnionych.

c) W przypadku bezczynności użytkownika na stacji roboczej trwającej więcej niż 10 min, uruchamiany jest automatycznie wygaszacz ekranu. Wznowienie pracy możliwe jest po ponownym uwierzytelnieniu się poprzez podanie własnego hasła.

3) Stosowane są następujące zasady zakończenia pracy w systemie informatycznym:
a) Po zakończeniu pracy należy wylogować się z systemu.
b) Po zakończeniu dnia pracy użytkownik zobowiązany jest do zabezpieczenia wszelkich dokumentów i nośników zawierających dane osobowe, w celu uniemożliwienia dostępu do nich osób nieupoważnionych. Należy uprzątnąć z miejsca pracy wszelkie dokumenty, nośniki, notatki i umieścić je w miejscu niedostępnym dla osób nieupoważnionych.

6. Zabezpieczenie nośników informacji zawierających dane osobowe

1) Przekazywanie, niszczenie nośników zawierających dane osobowe:
a) Nośniki danych przeznaczone do likwidacji należy wcześniej pozbawiać zapisanych danych w sposób uniemożliwiający ich odzyskanie lub uszkodzone, w taki sposób aby odczyt danych stał się niemożliwy.
b) Z urządzeń i/lub nośników danych zawierających dane osobowe przed przekazaniem podmiotowi nieuprawnionemu należy te dane usunąć w sposób trwały uniemożliwiający późniejsze ich odczytanie/odtworzenie.
c) Z urządzeń i/lub nośników danych zawierających dane osobowe przed przekazaniem do naprawy należy usunąć te dane w sposób trwały uniemożliwiający późniejsze odczytanie/odtworzenie lub naprawiać w obecności osoby upoważnionej.
d) Dopuszcza się przekazanie nośników danych bez usunięcia danych osobowych jedynie w przypadku przekazywania ich specjalistycznej firmie w celu odzyskania danych. W takiej sytuacji wymagane jest zobowiązanie firmy zewnętrznej do podpisania umowy powierzenia danych osobowych.
e) Transport nośników zawierających dane osobowe poza granice obszarów przetwarzania firmy powinien być dokonywany w sposób uniemożliwiający uzyskanie dostępu do nich przez osoby nieuprawnione.
f) W przypadku konieczności przesyłania danych wymaga się ich wcześniejsze zabezpieczenie przed dostępem dla osób nieupoważnionych.
g) Transport nośników zawierających dane osobowe poza granice obszarów przetwarzania firmy powinien być dokonywany z zachowaniem szczególnej uwagi, tak aby nośnik informacji nie został zgubiony, skradziony lub uszkodzony. W przypadku zlecania transportu nośników danych należy korzystać z godnego zaufania transportu i kurierów.
h) Zabrania się wynoszenia nośników danych poza obszar zidentyfikowany jako obszar przetwarzania danych bez zgody Administratora danych osobowych..
2) Przechowywanie nośników danych:
a) W przypadku przechowywania danych osobowych (nośników) poza obszarem wyznaczonym jako obszar przetwarzania danych osobowych, dane te powinny być zabezpieczone środkami dodatkowymi w celu zachowania poufności i integralności .
b) Nośniki danych (w tym również kopie zapasowe i archiwalne) należy przechowywać w wydzielonym pomieszczeniu i/lub szafie/sejfie w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
c) Warunki środowiskowe przechowywania nośników są zgodne z wytycznymi producentów nośników.
d) Kopie zapasowe usuwa się (niszczy) niezwłocznie po ustaniu ich użyteczności.
e) W przypadku jeśli dostęp do nośników ma więcej niż jedna osoba zaleca się, aby wprowadzony system kontroli dostępu zapewniał identyfikacje, autoryzację oraz rozliczalność osoby.

7. Kopie zapasowe

1) Wszystkie dane osobowe przetwarzane w systemie informatycznym firmy są zachowywane w kopiach zapasowych.
2) Kopie zapasowe tworzy się w taki sposób, aby zapewnić odtworzenie wszystkich informacji w przypadku awarii.
3) Kopią zapasową objęte są:
a) bazy danych zawierających zbiory danych osobowych;
b) programy i narzędzia programowe służące do przetwarzania danych;
c) pozostałe zasoby zawierające dane osobowe.

8. Zabezpieczenie systemu informatycznego przed działalnością nieuprawnionego oprogramowania

1) Administrator Systemów Informatycznych jest zobowiązany do wprowadzenia obligatoryjnej ochrony antywirusowej, a także zabezpieczenia zaporą sieciową, która obejmuje wszystkie stacje robocze oraz serwery.
2) Oprogramowanie antywirusowe powinno być skonfigurowane w sposób wymuszający automatyczne usuwanie wirusów, zaś w przypadku gdy ich usunięcie jest niemożliwe, obejmowanie ich kwarantanną, okresowe skanowanie wszystkich dysków lokalnych, a także sporządzanie raportów oraz powiadamianie osoby odpowiedzialnej o wykrytych wirusach, robakach czy innym szkodliwym oprogramowaniu.
3) Dokonywanie zmian w konfiguracji oprogramowania antywirusowego oraz zapory sieciowej jest możliwa tylko przez Administratora Systemów Informatycznych.
4) Przeprowadzane są okresowe szkolenia z zakresu bezpiecznej pracy z aplikacjami wykorzystywanymi na stacjach roboczych ze szczególnym uwzględnieniem aplikacji wykorzystywanych do łączności z sieciami zewnętrznymi (np: przeglądarka internetowa, klient poczty itp.) Szkolenia powinny uświadamiać użytkownikom skalę i typy zagrożeń oraz metody jak ich uniknąć lub obniżyć prawdopodobieństwo infekcji.
5) Użytkownicy zobowiązani są do sprawdzania programem antywirusowym wszelkich elektronicznych zewnętrznych nośników informacji.

9. Wykonywanie przeglądów i konserwacji systemów informatycznych

1) Administrator Systemów Informatycznych wykonuje przeglądy i konserwacje systemów informatycznych zgodnie z terminami określonymi przez producentów sprzętu lub oprogramowania lub zgodnie z harmonogramem określonym przez Administratora danych osobowych.
2) Administrator Systemów Informatycznych jest zobowiązany do prowadzenia dokumentacji dotyczącej przeprowadzanych przeglądów i konserwacji systemu informatycznego.
Dokumentacja ta powinna zawierać w szczególności:
a) czas i datę rozpoczęcia przeglądu lub konserwacji;
b) zakres wykonanych prac;
c) wykaz osób przeprowadzających przegląd lub konserwację;
d) czas i datę zakończenia przeglądu lub konserwacji.
3) Wszelkie prace serwisowe i konserwacyjne systemu informatycznego wykonywane przez podmiot zewnętrzny może odbywać się na zasadach określonych w umowie z uwzględnieniem klauzuli dotyczącej ochrony danych osobowych.

4) Wszelkie informacje, dane, oprogramowanie, sprzęt udostępniane firmom lub instytucjom zewnętrznym muszą zostać zabezpieczone przed dostępem osób niepowołanych poprzez: zabezpieczenie fizyczne przed uszkodzeniem, zachowanie zasad ochrony informacji, zachowanie zasad ochrony fizycznej i mienia.
5) Wszelkie prace serwisowe i konserwacyjne systemu informatycznego wykonywane doraźnie przez podmiot zewnętrzny mogą być wykonywane wyłącznie w obecności Administratora danych osobowych lub osoby upoważnionej do przetwarzania danych.
6) Rozpoczęcie prac serwisowych lub konserwacyjnych systemu informatycznego przez podmiot zewnętrzny poprzedzone jest wcześniejszą informacją o zakresie planowanych prac. Prace mogą zostać rozpoczęte nie wcześniej niż po akceptacji przedstawionego zakresu prac przez Administratora danych osobowych.
7) Przed rozpoczęciem prac serwisowych lub konserwacji systemu informatycznego przez podmiot zewnętrzny, konieczne jest potwierdzenie tożsamości serwisantów przez Administratora danych osobowych lub osobę upoważnioną do przetwarzania danych.