



Szkoła Podstawowa nr 1 Adama Mickiewicza w Radzionkowie

SZKOŁA PODSTAWOWA NR 1

im. Adama Mickiewicza

41-922 Radzionków

ul. ks. dr J. Knosały 16

NIP 645-22-23-457

ZARZĄDZENIE

wewnętrzne nr 8 / 2019

Dyrektora Szkoły Podstawowej nr 1 im. Adama Mickiewicza
w Radzionkowie

z dnia 12 marca 2019 r.

w sprawie wprowadzenia Instrukcji Zarządzania Systemem Informatycznym

Na podstawie

art. 24 Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej (UE) 2016/679 z dnia 27 kwietnia 2016 r.
w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu
takich danych oraz uchylenia dyrektywy 95/46/WE

Dyrektor

Szkoły Podstawowej nr 1 im. Adama Mickiewicza

zarządza, co następuje:

§ 1

Wprowadza się:

„Instrukcję Zarządzania Systemem Informatycznym”

w Szkole Podstawowej nr 1 im. Adama Mickiewicza w Radzionkowie - stanowiącą załącznik do niniejszego zarządzenia

§ 2. Zarządzenie wchodzi w życie z dniem podpisania

§ 3. Zarządzenie podlega ogłoszeniu na tablicach ogłoszeń Szkoły Podstawowej nr 1 im. Adama Mickiewicza.

DYREKTOR
Szkoły Podstawowej nr 1
w Radzionkowie
mgr Marek Napieraj

Dyrektor Szkoły Podstawowej nr 1

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Szkoła Podstawowa nr 1 im. Adama Mickiewicza w Radzionkowie

Niniejsza Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych Szkoły Podstawowej nr 1 im. Adama Mickiewicza w Radzionkowie przetwarzane są w sposób zgodny z przepisami prawa mają zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust.2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016r. w sprawie ochrony danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej RODO).

Definicje:

1. Administrator Danych – Szkoła Podstawowa nr 1 z siedzibą w Radzionkowie ul. Knosały 16, 41-922 Radzionków, NIP 645-22-23-457 reprezentowana przez Dyrektora Szkoły – Marka Napieraj.
2. Dane osobowe – wszelkie informacje, w tym o stanie zdrowia, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
3. System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
4. Użytkownik – osoba upoważniona przez Administratora Danych do Przetwarzania Danych Osobowych w Szkole Podstawowej nr 1 w Radzionkowie.
5. Sieć lokalna – połączenie Systemów Informatycznych Administratora Danych wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych
6. Zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
7. Przetwarzane danych – jakiegokolwiek operacje wykonywane na danych osobowych, takiej jak zbieranie, utrwalanie, przechowywanie, opracowanie, zmienianie, udostępnienie i usuwanie, a zwłaszcza te, które wykonuje w Systemach informatycznych.
8. Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionymi Przetwarzaniem.
9. Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w Systemie informatycznym (Użytkownikowi).

I.

Procedury nadawania upoważnień do Przetwarzania danych

1. Za bezpieczeństwo Danych osobowych w Systemie informatycznym i za właściwy nadzór odpowiedzialny jest Administrator Danych.
2. Do obsługi Systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do Przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie wydane przez Administratora Danych,
3. Szkoła prowadzi Rejestr osób posiadających upoważnienie do przetwarzania danych osobowych.

II.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez Użytkowników systemu

1. Pracownik po przyjsciu do pracy uruchamia stację roboczą (komputer, laptop itp...).
2. Przed uruchomieniem komputera należy sprawdzić, czy nie zostały do niego podłączone żadne niezidentyfikowane urządzenia.

3. W trakcie pracy przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane Dane osobowe.
4. Przy opuszczaniu stanowiska na dłuższy czas należy ustawić ręcznie blokadę klawiatury i wygaszacz ekranu (wygaszacz nie rzadszy niż aktywujący się po 15 minutach braku aktywności).

III.

Tworzenie kopii zapasowych Zbiorów danych

1. Dla zabezpieczenia integralności danych dokonuje się archiwizacji danych w systemach Szkoły Podstawowej nr 1 im. Adama Mickiewicza w Radzionkowie.
2. Do archiwizacji służą płyty DVD oraz pendrive z zapisem danych z systemu
3. Wszystkie dane archiwizowane winny być identyfikowane, tj. zawierać takie informacje jak datę dokonania zapisu oraz identyfikator zapisanych w kopii danych.

IV.

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

1. Nośniki z kopiami archiwalnymi powinny być zabezpieczone przed dostępem do nich osób nieupoważnionych, przed zniszczeniem czy kradzieżą.
2. Nośników z danymi zarchiwizowanymi nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są Zbiory danych osobowych używane na bieżąco.
3. Nośniki informacji, kopie zapasowe, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.
4. Kopie, które są już nieprzydatne, należy zniszczyć fizycznie lub stosując wymazywanie poprzez wielokrotny zapis nieistotnych informacji w obszarze zajmowanym przez dane kasowane.
5. Zabrania się wynoszenia jakichkolwiek nagranych nośników zawierających dane osobowe z miejsca pracy.

V.

Sposób zabezpieczenia Systemu informacyjnego przed działalnością wirusów komputerowych, nieuprawnionym dostępem oraz awariami zasilania

1. System informatyczny jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu oraz przed działaniami inicjowanymi z sieci zewnętrznej.

Zabezpieczenie obejmuje:

	Obszar chroniony	Rodzaj ochrony
1.	Stacje robocze	System antywirusowy
2.		Firewall
3.		Szyfrowanie nośników danych
4.	Sieć wewnętrzna	System antywirusowy
5.		Firewall
6.	Poczta e-mail	Szyfrowanie danych
7.		System antywirusowy i antyspamowy

2. Użytkowane w systemie komputery są automatycznie skanowane.
3. Aktualizacja bazy wirusów odbywa się poprzez automatyczne pobieranie bazy wirusów przez program antywirusowy.
4. W przypadku wykrycia wirusa należy:
 - a) uruchomić program antywirusowy i skontrolować użytkowany system,
 - b) usunąć wirusa z systemu przy wykorzystaniu programu antywirusowego.

Jeżeli operacja usunięcia wirusa się nie powiedzie, należy:

- a) zakończyć pracę w systemie komputerowym,
 - b) odłączyć zainfekowany komputer z sieci,
 - c) powiadomić o zaistniałej sytuacji Administratora Danych lub ASI
5. Urządzenia i nośniki zawierające Dane osobowe przekazywane poza obszar, w którym są one przetwarzane, zabezpiecza się w sposób zapewniający poufność i integralność danych.

VI.

Poczta elektroniczna

1. Pracownicy mogą korzystać z poczty elektronicznej w celach służbowych oraz w celach prywatnych w zakresie ograniczonym swoimi obowiązkami.
2. Administrator może poznawać treść wiadomości elektronicznych wykorzystywanych przez pracowników znajdujących się we wszystkich systemach Administratora.
3. Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem (tzw. phishing email). W szczególności zabronione jest otwieranie linków bądź pobieranie plików zapisanych w komunikacji zewnętrznej od nieznanego nadawcy.

VIII.

Procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do Przetwarzania danych

1. Przeglądy kontrolne, serwis sprzętu i oprogramowania powinny być dokonywane przez firmy serwisowe, z którymi zostały zawarte umowy zawierające postanowienia zobowiązujące je do przestrzegania zasad poufności informacji uzyskanych w ramach wykonywanych zadań.
2. Przy dokonywaniu serwisu należy przestrzegać następujących zasad:
 - a) czynności serwisowe powinny być wykonywane w obecności osoby upoważnionej do Przetwarzania danych, Instrukcja zarządzania systemem informatycznym,
 - b) przed rozpoczęciem tych czynności dane i programy znajdujące się w systemie powinny zostać zabezpieczone przed ich zniszczeniem, skopiowaniem lub niewłaściwą zmianą,
 - c) prace serwisowe należy ewidencjonować w książce zawierającej rodzaj wykonywanych czynności serwisowych, daty rozpoczęcia i zakończenia usługi, odnotowanie osób dokonywujących czynności serwisowych, tj. imienia i nazwiska, a także osób uczestniczących w pracach serwisowych,
 - d) w przypadku prac serwisowych dokonywanych przez podmiot zewnętrzny, wymagających dostępu do Danych osobowych, z podmiotem takim powinny zostać zawarte stosowne umowy powierzenia danych osobowych.

Dyrektor Szkoły Podstawowej nr 1