**ZARZĄDZENIE NR 11/2018**

**DYREKTORA SZKOŁY PODSTAWOWEJ NR 2 IM. JANA KILIŃSKIEGO**

**W KROŚNIE ODRZAŃSKIM**

**z dnia 8 maja 2018 r.**

w sprawie**: wprowadzenia Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym**

Na podstawie : Rozporządzenia Parlamentu Europejskiego i Rady (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 (dalej: RODO)
Oraz § 3 ust. 3 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 zarządza się, co następuje:

**§ 1**

Przyjmuje się do stosowania „Politykę bezpieczeństwa" oraz ,,Instrukcję zarządzania systemem informatycznym", stanowiącą załącznik Nr 1 do niniejszego zarządzenia.

**§ 2**

1. Wykonanie zarządzenia powierza się pracownikom Szkoły podstawowej nr 2 im. Jana Kilińskiego w Krośnie Odrzańskim.
2. Wszyscy pracownicy potwierdzają własnoręcznym podpisem fakt zapoznania się z treścią niniejszego zarządzenia.
3. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1 do Zarządzenia nr 11/2018
z dnia 8 maja 2018 r
w sprawie wprowadzenia polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym

# INSTRUKCJA
# ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

# ROZDZIAŁ I
# Postanowienia ogólne

**§ 1**

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją”, określa sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji, a także zasady i tryb postępowania Administratora Danych oraz osób przez niego upoważnionych przy przetwarzaniu danych osobowych.

2. Instrukcja została opracowana w celu realizacji wymogów określonym w §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 na poziomie wysokim.

**§ 2**

Instrukcja określa stosowne procedury i warunki zarządzania systemem informatycznym oraz kartotekami, zapewniającymi ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

**§ 3**

Ilekroć w Instrukcji mowa jest o:

1) zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
2) przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje systemach informatycznych,

3) systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4) kartotece – rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierającej dane osobowe,
5) Administratorze Danych – rozumie się przez to Szkołę Podstawową nr 2 im. Jana Kilińskiego w Krośnie Odrzańskim,
6) Dyrektorze – rozumie się przez to Dyrektora Szkoły Podstawowej nr 2 im/ Jana Kilińskiego w Krośnie Odrzańskim
7) Inspektorze Ochrony Danych Osobowych – rozumie się przez to osobę nadzorującą przestrzeganie zasad ochrony przetwarzanych danych osobowych. Nadzoruje on stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych , a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz zmianą utratą, uszkodzeniem lub zniszczeniem, a także przeprowadza kontrole w zakresie określonym regulacjami wewnętrznymi Administratora danych,
8) osobie odpowiedzialnej za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację – rozumie się przez to osobę wyznaczoną przez dyrektora szkoły,
9) komórce organizacyjnej – rozumie przez to każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną, zgodnie z regulaminem organizacyjnym,
10) użytkowniku – rozumie się przez to osobę wykonującą zadania w systemie informatycznym oraz kartotekach,
11) pomieszczeniach – rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego, przenośnego sprzętu komputerowego lub gromadzone w kartotekach

**§ 4**

Realizację prawidłowego przetwarzania danych osobowych zagwarantują następujące założenia:

1) wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania danych osobowych oraz ich odpowiedzialność za ochronę tych danych,

2) przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,

3) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory) oraz zapewniających dostęp użytkowników do różnych poziomów zbiorów danych osobowych – stosownie do indywidualnego zakresu upoważnienia,

4) podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,

5) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,

6) opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii,

7) śledzenie osiągnięć w dziedzinie zabezpieczania systemów informatycznych i - w miarę możliwości organizacyjnych i techniczno-finansowych – wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemem informatycznym, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

## ROZDZIAŁ II
## Przydział uprawnień i identyfikatorów

**§ 5**

1. Każdy użytkownik dopuszczony do przetwarzania danych osobowych posiada stosowne upoważnienie. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 1 do Instrukcji.
2. Każdy użytkownik posiada indywidualny identyfikator umożliwiający logowanie do tych aplikacji, z którymi może pracować.
3. Identyfikator umożliwia wykonanie czynności zgodnie z zakresem powierzonych obowiązków, które wyznaczają poziom uprawnień.

4. Postanowienia ust. 2 dotyczą użytkowników, którzy jako jedyni mają dostęp do danych przetwarzanych w systemie informatycznym oraz użytkowników, którzy mają dostęp wyłącznie do danych osobowych gromadzonych w kartotekach.
5. Dyrektor szkoły jako administrator danych osobowych prowadzi ewidencję przyznanych poszczególnym użytkownikom uprawnień związanych z dostępem do zbiorów danych oraz dokonywaniem zmian w zakresie przyznanych uprawnień.
6.

**§ 6**

Do uwierzytelniania użytkowników w systemie używa się haseł lub innych metod zapewniających weryfikację tożsamości użytkownika.

**§ 7**

Każdy użytkownik zobowiązany jest do zachowania w tajemnicy własnych haseł, także po upływie ich ważności.

**§ 8**

1. Identyfikator dla użytkowników upoważnionych do przetwarzania danych osobowych w systemie informatycznym, niezbędne do logowania się do określonej aplikacji, ustala i przydziela Dyrektor szkoły jako administrator danych osobowych lub wyznaczona przez dyrektora osoba .
2. Identyfikator użytkownika nie podlega zmianie.
3. Identyfikator użytkownika podlega rejestracji w systemie informatycznym.

**§ 9**

1. Pierwsze hasło użytkownika ustala Administrator Danych przy wprowadzaniu identyfikatora użytkownika systemu.
2. Hasła muszą odpowiadać następującym wymogom:

a) dla poziomu bezpieczeństwa podstawowego 6 znaków,

b) nie mogą być zapisywane w systemie w postaci jawnej,

c) nie mogą być w nich używane imiona, nazwiska, przezwiska, inicjały i inne kombinacje znaków mogących doprowadzić do łatwego rozszyfrowania haseł przez osoby nieupoważnione,

d) nie mogą być w nich stosowane wyłącznie znaki następujące po sobie na klawiaturze bądź te same litery czy cyfry.

**§ 10**

1. Po otrzymaniu hasła użytkownik zobowiązany jest zalogować się do systemu i powinien zmienić hasło. Przy wpisaniu hasło nie może być wyświetlane na ekranie.
2. Hasło zmieniane jest nie rzadziej niż co 30 dni. Za systematyczną, terminową zmianę hasła odpowiada użytkownik.

**§ 11**

Hasło podlega natychmiastowej zmianie w przypadku podejrzenia jego odkrycia przez nieupoważnioną osobę.

**§ 12**

1. Hasła nie mogą być nigdzie zapisywane, z wyjątkiem haseł Administratora, które przechowywane są w opieczętowanych kopertach, w miejscu wyznaczonym przez Inspektora Ochrony Danych Osobowych.
2. Tryb przechowywania i udostępniania haseł Administratora określa załącznik nr 2 do Instrukcji.

## ROZDZIAŁ III
## Rejestrowanie i wyrejestrowanie użytkowników

**§ 11**

1. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Administrator Danych.
2. Ewidencja użytkowników może być prowadzona w systemie informatycznym.

**§ 12**

Nośniki magnetyczne (optyczne), na których gromadzone są wykazy zawierające ewidencje użytkowników przechowywane są w wyznaczonych szafach lub sejfach, do których dostęp ma wyłącznie Administrator Danych oraz Inspektor Ochrony Danych Osobowych.

**§ 13**

Zmiany dotyczące użytkownika sieci, takie jak:

1) zmiana imienia lub nazwiska,

2) zmiana zakresu upoważnienia,

podlegają niezwłocznemu odnotowaniu w ewidencji.

**§ 14**

1. Zmiany dotyczące użytkownika, takie jak:
   1) rozwiązanie umowy o pracę,
   2) utrata upoważnienia do przetwarzania danych osobowych,
   3) zmiana zakresu obowiązków służbowych skutkująca ustaniem upoważnienia,

   powodują wyrejestrowanie użytkownika przez Administratora, w trybie natychmiastowym z ewidencji, zablokowanie identyfikatora oraz unieważnienie hasła tego użytkownika.

**§ 15**

1. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.
2. Osoba prowadząca ewidencję obowiązana jest odrębnie gromadzić identyfikatory, które utraciły ważność lub też stosować odpowiednie ich oznaczenia.

## ROZDZIAŁ IV
## Procedury rozpoczęcia, zawieszenia i zakończenia pracy

**§ 16**

Przed przystąpieniem do pracy z systemem informatycznym lub kartotekami, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz dokonać oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie poufności danych osobowych.

**§ 17**

W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie systemu, użytkownik obowiązany jest poinformować przełożonego.

**§ 18**

1. Rozpoczynając pracę na komputerze użytkownik loguje się do systemu informatycznego.
2. Użytkownik wprowadza identyfikator i dokonuje uwierzytelnienia.

3. Jeśli system umożliwia, po przekroczonej liczbie prób logowania system blokuje dostęp do systemu informatycznego na poziomie danego użytkownika.
4. Użytkownik ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania. O zaistniałym incydencje powiadamia Administratora Danych lub osobę przez niego wyznaczoną.

**§ 19**

Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest wylogować się z sytemu informatycznego.

**§ 20**

Kończąc pracę należy:

1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
2) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, przed dostępem osób nieuprawnionych.

## ROZDZIAŁ V
## Procedury tworzenia kopii zapasowych

**§ 21**

1. Zbiory danych osobowych oraz programy i narzędzia programowe służące do ich przetwarzania, zapisywane na nośnikach zewnętrznych (streamer, dyski: wymienne, magnetyczne, optyczne) tworzące kopie zapasowe kolejnych okresów, powinny być odpowiednio oznakowane i przechowywane w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach.
2. Kopie zapasowe określone w ust. 1 niniejszego paragrafu powinny być sporządzane regularnie.
3. Za prawidłowe sporządzanie kopii zapasowych, ich oznakowanie i przechowywanie, odpowiedzialny jest Administrator Danych Osobowych
4. Odpowiada on również za sprawdzanie poprawności wykonania kopii zapasowych na nośnik zewnętrzny.

**§ 22**

1. Użytkownicy obowiązani są przestrzegać terminów tworzenia doraźnych kopii zapasowych, o ile zostali do tego upoważnieni przez Administratora.

2. Użytkownicy określeni w ust. 1 są odpowiedzialni za prawidłowe sporządzenie kopii zapasowych, ich oznakowanie i przechowywanie.

**§ 23**

1. Kopie zapasowe, które uległy uszkodzeniu lub ustała ich użyteczność podlegają natychmiastowemu zniszczeniu z zachowaniem procedur określonych niniejszą Instrukcją.
2. Zniszczenia kopii zapasowych, na nośnikach magnetycznych i optycznych dokonuje użytkownik w obecności Administratora lub osoby przez niego wyznaczonej.
3. Z nośników magnetycznych i optycznych wielokrotnego użytku np. CDRW dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku, gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym odzyskanie danych.
4. Dane zawarte na nośnikach jednokrotnego użytku np. CDR należy usuwać poprzez całkowite zniszczenie nośnika.

# ROZDZIAŁ VI
# Przetwarzanie danych osobowych

**§ 24**

1. Dane osobowe przetwarzane są w kartotekach oraz w komputerach do tego przeznaczonych (serwerach, stacjach roboczych) zlokalizowanych w obszarach przetwarzania danych osobowych.
2. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.
3. Szczegółowy opis obszaru przetwarzania danych osobowych oraz środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności danych osobowych określony jest w Polityce bezpieczeństwa.

**§ 25**

Decyzje o likwidacji zbiorów danych osobowych, przetwarzanych w kartotekach oraz systemach informatycznych podejmuje Administrator Danych.

**§ 26**

Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych, Administrator Danych lub osoba przez niego upoważniona sporządza protokół , w którym zamieszcza następujące informacje:

1. datę dokonania likwidacji,
2. przedmiot likwidacji,
3. przedział czasowy likwidowanych zbiorów danych osobowych,
4. podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.

# ROZDZIAŁ VII
# Zabezpieczenie systemu informatycznego

**§ 27**

System informatyczny zabezpiecza się przed:

1. działaniem, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
2. utratą danych spowodowanych:
    a) działaniem nielegalnego oprogramowania,
    b) awarią zasilania lub zakłóceniami w sieci zasilającej.

**§ 28**

1. Administrator lub osoba przez niego wyznaczona odpowiada za niezwłoczne instalowanie na sprzęcie najnowszych wersji oprogramowania zabezpieczającego system informatyczny.
2. Nowe wersje oprogramowania instaluje wyłącznie Administrator niezwłocznie po ich otrzymaniu lub osoba upoważniona przez Administratora.
3. Okresowych kontroli w zakresie instalowania najnowszych wersji oprogramowania zabezpieczającego system informatyczny dokonuje Inspektor Ochrony Danych Osobowych lub osoba przez niego upoważniona.

**§ 29**

1. Na serwerach i stacjach roboczych używanych przez Administratora Danych powinno instalować się przynajmniej jeden program antywirusowy.
2. Program antywirusowy należy również instalować na komputerach przenośnych.

**§ 30**

W komputerach przenośnych zawierających dane osobowe stosuje się środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

**§ 31**

1. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie informatycznym, jak i do celów informacyjnych.
2. Na serwerach, w miarę możliwości technicznych, oprogramowanie antywirusowe powinno być aktywne cały czas.
3. Na stacjach roboczych oprogramowanie antywirusowe powinno być aktywne cały czas i powinno dokonywać sprawdzenia każdego otwieranego lub uruchomianego pliku.

**§ 32**

Użytkownicy są zobowiązani do dokonywania kontroli antywirusowej wszystkich nośników magnetycznych lub optycznych przychodzących z zewnątrz oraz okresowo nośników własnych.

**§ 33**

1. W razie stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Administratora.
2. Administrator lub osoba przez niego wyznaczona usuwa wirusa, jeśli automatycznie nie dokonał tego program antywirusowy oraz informuje Inspektora Danych Osobowych lub osobę przez niego upoważnioną o dokonanych czynnościach i rodzaju wirusa.

**§ 34**

W razie niemożności usunięcia wirusa, Administrator może skorzystać z usług zewnętrznych specjalistów w tej dziedzinie.

**§ 35**

1. W sytuacji korzystania z usług zewnętrznych specjalistów należy podjąć działania uniemożliwiające tym osobom dostęp do danych osobowych.
2. Prace określone w ust. 1 są wykonywane pod nadzorem Administratora Danych lub upoważnionego użytkownika i w miarę możliwości bez dostępu do danych osobowych.

**§ 36**

1. Administrator Danych jest odpowiedzialny za kontrole antywirusowe serwerów i zasobów sieciowych.
2. Użytkownicy są odpowiedzialni za kontrole antywirusowe na dyskach lokalnych i innych nośnikach.

**§ 37**

1. Po usunięciu wirusa Administrator Danych sprawdza zainfekowany system informatyczny oraz przywraca go do pełnej sprawności i funkcjonalności.
2. Administrator sporządza raport o wystąpieniu wirusa. Raport powinien zawierać następujące informacje:
    1) nazwę wirusa,
    2) datę wykrycia wirusa,
    3) miejsce zainfekowania,
    4) źródło infekcji.
3. Raport, o którym mowa w ust. 2 przekazywany jest Inspektorowi lub osobie przez niego wyznaczonej wraz z wnioskami, stosownymi do zaistniałej sytuacji.

**§ 38**

1. Przy przetwarzaniu danych osobowych zakwalifikowanych do poziomu bezpieczeństwa wysokiego system informatyczny służący do przetwarzania danych osobowych chroni przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:
    1) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną,
    2) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
3. Wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej stosuje się środki ochrony kryptograficznej.

**§ 39**

Administrator prowadzi wykaz przypadków zainfekowania komputerów i nośników wykorzystywanych do przetwarzania danych osobowych w systemie oraz przechowuje kopie raportów.

**§ 40**

Procedura wyrażona w niniejszym rozdziale ma zastosowanie także do przypadków awarii systemu spowodowanych błędem programu bądź użytkownika.

## ROZDZIAŁ VIII
## Wymagania dotyczące sprzętu i oprogramowania

**§ 41**

1. Sprzęt obsługujący zbiór danych osobowych składa się z komputerów stacjonarnych klasy PC oraz komputerów przenośnych.
2. Komputery przenośne mogą być używane do przetwarzania danych osobowych po odpowiednim ich zabezpieczeniu.
3. Użytkownik korzystający z komputera przenośnego jest zobowiązany do zachowania szczególnej ostrożności podczas transportu komputera oraz nie może udostępnić komputera osobom nieupoważnionym.
4. Komputer przenośny nie może być transportowany bez wiedzy Administratora Danych Osobowych.
5. Komputer przenośny należy przechowywać tylko i wyłącznie w pomieszczeniach Szkoły, z wyjątkiem komputera służbowego dyrektora Szkoły.
6. Na okres wakacji i dni wolnych należy zabezpieczyć komputery przenośne zgodnie z wytycznymi Administratora Danych Osobowych.Za zabezpieczenie każdego przenośnego komputera odpowiada użytkownik.

**§ 42**

1. Sieć komputerowa służąca do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilane energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu komputerowego.
2. Oprogramowanie każdego komputera powinno zapewnić bezpieczne wyłączanie systemu informatycznego, po dokonaniu operacji zamknięcia w pracujących aplikacjach i oprogramowaniu systemowym.

3. Serwer sieci powinien być zasilany przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie napięcia przez min. 15 minut oraz na wykonanie bezpiecznego wyłączenia serwera, tak aby przed zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na zbiorze danych osobowych.

**§ 43**

1. Za prawidłowe zasilanie energetyczne sieci komputerowej odpowiedzialny jest pracownik obsługujący sieć.
2. Infrastruktura techniczna związana z siecią komputerową i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.
3. Wszystkie urządzenia w sieci komputerowej (pozostałe stacje robocze, drukarki, modemy itd.) powinny być w miarę możliwości technicznych włączone do sieci energetycznej, zapewniającej odpowiednie uziemienie i zabezpieczenie przed przepięciami.
4. Gniazda zasilania sieci komputerowej powinny być odpowiednio oznakowane, zabezpieczone przed włączeniem do nich odbiorników lub wykonane w specjalnym standardzie.

**§ 44**

1. Dane osobowe przesyłane na nośnikach magnetycznych i optycznych oraz za pomocą systemów teleinformatycznych powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.
2. Dane osobowe przesyłane na łączach telekomunikacyjnych wewnątrz danej sieci powinny być dodatkowo zabezpieczone w sposób uniemożliwiający dostęp do danej sieci LAN z innej sieci.

**§ 45**

1. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.
2. Uprawnienie do instalowania programów na komputerach służbowych posiada wyłącznie Administrator lub osoba przez niego upoważniona.

**§ 46**

Administrator odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelnienia użytkownika oraz za sprawowanie kontroli dostępu do danych osobowych jedynie osób upoważnionych.

**§ 47**

1. Administrator Danych Osobowych odpowiedzialny jest za to, aby dla każdej osoby, której dane osobowe są przetwarzane, system informatyczny zapewniał odnotowanie:
   1) daty pierwszego wprowadzenia danych do systemu,
   2) identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,
   3) źródła danych, w przypadku zbierania danych nie od osoby, które one dotyczą,
   4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych,
   5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych.

   Wymagania określone w niniejszym ustępie nie dotyczą systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie.
2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust.1.
4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą

być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

5. Do czasu spełnienia przez system informatyczny wszystkich wyżej wymienionych wymogów, system informatyczny powinien zapewnić odnotowanie:
   1) daty pierwszego wprowadzenia danych,
   2) identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.

6. Do chwili spełnienia przez system informatyczny wszystkich wymogów określonych w niniejszym paragrafie, odnotowanie informacji określonych w ust. 1 pkt. 3, 4 i 5 należy prowadzić w formie tradycyjnej (papierowej) lub komputerowo poza systemem.

## ROZDZIAŁ IX
## Procedury wykonywania przeglądów i konserwacji

**§ 48**

1. Bieżących oraz okresowych przeglądów, napraw i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych, niewymagających angażowania zewnętrznych firm serwisowych, dokonuje Administrator lub osoba przez niego wyznaczona.
2. Przeglądów i konserwacji zbiorów danych osobowych dokonują użytkownicy, zgodnie z indywidualnymi zakresami upoważnień i odpowiedzialności.

**§ 49**

Prace dotyczące przeglądów, konserwacji i napraw, wymagające zaangażowania firm zewnętrznych, są wykonywane za wiedzą Inspektora Ochrony Danych Osobowych przez uprawnionych przedstawicieli tych firm pod nadzorem Administratora lub upoważnionego użytkownika i w miarę możliwości bez dostępu do rzeczywistych danych osobowych.

**§ 50**

1. W przypadku, gdy zaistnieje potrzeba naprawy lub wymiany sprzętu komputerowego służącego do przetwarzania lub przechowywania danych osobowych, należy usunąć dane, w sposób uniemożliwiający ich odzyskanie.

2. Jeżeli nie ma możliwości usunięcia danych należy urządzenie uszkodzić w sposób uniemożliwiający ich odczytanie.

**§ 51**

Nadzór nad instalowaniem, sprawnym funkcjonowaniem i wymianą uszkodzonych urządzeń oraz ich likwidacją sprawuje Inspektor Ochrony Danych Osobowych lub osoba wyznaczona przez Administratora .

## ROZDZIAŁ X
## Kontrola użytkowników systemów komputerowych

**§ 52**

1. Wyłączne uprawnienia do instalowania, wymiany uszkodzonych urządzeń oraz ich likwidacji posiada Administrator Danych Osobowych lub osoba przez niego wyznaczona.
2. Do przetwarzania danych osobowych mogą być wykorzystywane wyłącznie komputery służbowe.
3. Administrator umożliwia pracownikom korzystanie z sieci internet w celu wykonywania zadań służbowych .
4. Korzystanie z sieci internet w innym celu jest zabronione.

## ROZDZIAŁ XI
## Postanowienia końcowe

**§ 53**

1. Użytkownik zobowiązany jest złożyć oświadczenie, o tym, iż został zaznajomiony z przepisami ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych oraz dokumentacją obowiązującą u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.
2. Wzór oświadczenia potwierdzającego zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych oraz dokumentacją obowiązującą u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania , stanowi załącznik nr 3 do Instrukcji.
3. Oświadczenia przechowywane są w aktach osobowych pracownika.

**Załącznik nr 1 do instrukcji zarządzania**
**Systemem informatycznym**

**……..**
**……..**

*(imię i nazwisko)* *(miejscowość, data)*

# UPOWAŻNIENIE

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t. j. Dz. U. z 2002r. Nr 101, poz. 926 ze zm.), oraz *Rozporządzenia Parlamentu Europejskiego i Rady (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 (dalej: RODO)*
upoważniam Panią*/Pana* do przetwarzania danych osobowych.

Upoważnienie obejmuje prawo wglądu, wprowadzania, modyfikowania i usuwania danych osobowych.

Zobowiązuję Panią*/Pana* do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych polityki bezpieczeństwa danych osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

…….

(podpis Administratora Danych)

*- niepotrzebne skreślić

**Załącznik nr 2 do instrukcji zarządzania systemem informatycznym**

# TRYB PRZECHOWYWANIA I UDOSTĘPNIANIA HASEŁ ADMINISTRATORA

Ustala się następujący tryb postępowania z hasłami Administratora:

1. Hasła Administratora przechowywane są w formie pisemnej w zabezpieczonej kopercie.
2. Koperta złożona jest w specjalnej szafie, do której dostęp posiada Dyrektor i osoby przez niego upoważnione.
3. Hasła, o którym mowa w pkt 1 dają najwyższe uprawnienia administratorskie do korzystania i obsługi systemu informatycznego.
4. Hasła zmieniane są co najmniej co 30 dni bądź natychmiast w przypadku podejrzenia odkrycia przez inną , nieupoważniona osobę.
5. Nowe, aktualne hasło zabezpiecza się według procedur opisanych w pkt 1 i 2.
6. Koperta wraz z hasłem, które straciło ważność podlega zniszczeniu przy użyciu niszczarki dokumentów.
7. Niszczenia, o których mowa w pkt 6 dokonuje Administrator w obecności osoby przez niego upoważnionej.
8. W sytuacjach awaryjnych zaistniałych pod nieobecność Administratora lub w razie jego niedyspozycji Sekretarz Szkoły udostępnia hasło osobie upoważnionej.

…….

(podpis Administratora Danych)

**Załącznik nr 3 do instrukcji zarządzania systemem informatycznym**

……..
……

*(imię i nazwisko)* *(miejscowość, data)*

# OŚWIADCZENIE

Oświadczam, iż zostałam*/zostałem* zaznajomiona*/zaznajomiony* z przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t. j. Dz. U. z 2002r. Nr 101, poz. 926 ze zm.),oraz *Rozporządzenia Parlamentu Europejskiego i Rady (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 (dalej: RODO)* wydanych na jej podstawie aktów wykonawczych oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych Polityka bezpieczeństwa danych osobowych oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Jednocześnie zobowiązuję się do ich przestrzegania.

……..

(podpis osoby składającej oświadczenie)

*- niepotrzebne skreślić

Załącznik nr 2 do Zarządzenia nr 11/2018
z dnia 8 maja 2018 r
w sprawie wprowadzenia Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym

# POLITYKA BEZPIECZEŃSTWA
# SZKOŁA PODSTAWOWA NR 2 IM. JANA KILIŃSKIEGO
# W KROŚNIE ODRZAŃSKIM

§ 1

Polityka bezpieczeństwa w zakresie ochrony danych osobowych gromadzonych i przetwarzanych w Szkole Podstawowej nr 2 im. Jana Kilińskiego w Krośnie Odrzańskim określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności przetwarzania danych, a także służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych.

§ 2

W dokumencie przyjmuje się następującą terminologię:

1. **Dane osobowe** – wszelkie dane, dzięki którym możliwe jest bez większego wysiłku zidentyfikowanie dowolnej osoby fizycznej. Należą do nich m.in.: imię i nazwisko, adres, numer PESEL.
2. **Dane wrażliwe** – dane osobowe objęte szczególną ochroną, dotyczące: pochodzenia rasowego lub etnicznego, poglądów politycznych i religijnych, przynależności związkowej, partyjnej lub wyznaniowej, stanu zdrowia, kodu genetycznego, nałogów, życia seksualnego, skazań, orzeczeń i mandatów. Danych tych nie przetwarza się.
3. **Ustawa o ochronie danych osobowych (UODO.)** – podstawowy akt prawny regulujący kwestie związane z gromadzeniem, przetwarzaniem i wykorzystywaniem danych osobowych. Jej podstawowym celem jest ochrona osób fizycznych, których dane narażone są na wykorzystywanie np. przez instytucje.
4. **Rozporządzenia Parlamentu Europejskiego i Rady (UE)** - **(RODO)** 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
5. **Administrator danych osobowych (ADO)** – podmiot, który decyduje w placówce o celach i środkach przetwarzania danych osobowych. W przypadku placówek oświatowych jest nim szkoła, reprezentowana przez dyrektora.
6. **Inspektor Ochrony Danych Osobowych**– osoba fizyczna, powołana przez administratora danych osobowych i odpowiada za ochronę oraz przetwarzanie danych osobowych w placówce.

7. **Urząd Ochrony Danych Osobowych (UODO)** – organ pełniący nadzór nad przestrzeganiem prawa w zakresie ochrony danych osobowych.
8. **Polityka bezpieczeństwa** – zestaw procedur dotyczących zarządzania systemami informacyjnymi w danej placówce.
9. **Incydent z zakresu ochrony danych osobowych** – każde działanie, które narusza przepisy ustawy o ochronie danych osobowych i jej aktów wykonawczych, bez względu na to, czy było dokonane świadomie lub nie.
10. **Przetwarzanie danych** – operacja lub zestaw operacji wykonywane na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, np. zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
11. **Naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

§ 3

Administrator danych powołuje Inspektora Ochrony Danych Osobowych w celu nadzorowania i przestrzegania zasad ochrony danych osobowych.

§ 4

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa załącznik 1.

§ 5

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa załącznik 2.

§ 6

Strukturę zbiorów danych wskazującą zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami określa załącznik 3.

§ 8

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez ADO , które prowadzą dokumentację opisującą sposób przetwarzania danych w podmiocie:

1. Ewidencję osób przetwarzających dane w podmiocie posiadających

upoważnienie.
2. Oświadczenie osoby przetwarzającej dane osobowe.
3. Zgody i odwołanie zgód na przebywanie w obszarze przetwarzania danych.

§ 9

Administrator Danych Osobowych jest obowiązany, poinformować wszystkie osoby, których dane osobowe są przetwarzane i gromadzone w Szkole Podstawowej nr 2 im. Jana Kilińskiego w Krośnie Odrzańskim, o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych wszelkich informacji.

§ 10

Administrator Danych Osobowych ma prawo powierzyć innemu podmiotowi przetwarzanie danych osobowych w drodze umowy zawartej na piśmie.

§ 11

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym określa Instrukcja Zarządzania Systemem Informatycznym.

§ 12

W sprawach nieuregulowanych w „Polityce Bezpieczeństwa" zastosowanie mają przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz *: Rozporządzenia Parlamentu Europejskiego i Rady (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 (dalej: RODO)*

§ 13

„Polityka Bezpieczeństwa" zaczyna obowiązywać z dniem 25 maja 2018r.

Administrator Danych Osobowych: ……
Data: ……