INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH W SZKOLE PODSTAWOWEJ W LECHOWIE

1. Cel instrukcji

2. Celem instrukcji jest określenie trybu postepowania w przypadku, gdy:
   1) stwierdzono naruszenie ochrony danych osobowych (działania naprawcze - uruchamiane w przypadku wystąpienia naruszenia danych),
   2) stwierdzono możliwość naruszenia ochrony danych osobowych (czynności profilaktyczne – stosowane w przypadku stwierdzenia, że doszło do incydentu, który nie skutkował naruszeniem ochrony danych).
3. Przykładem zdarzeń, które uruchamiają procedury opisane w instrukcji, są:
   1) stwierdzenie naruszenia zabezpieczenia systemu informatycznego,
   2) stwierdzenie, że stan urządzenia, zawartość zbioru danych, ujawnienie metod pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej, złamanie zabezpieczeń fizycznych oraz wystąpienie innych zdarzeń, może wskazywać na naruszenie zabezpieczenia danych osobowych.

2. Naruszenie zabezpieczenia systemu informatycznego

Naruszeniem zabezpieczeń systemu informatycznego jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, uszkodzenie lub zniszczenie danych osobowych lub jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1) złamanie kodów dostępu,
2) próba odkodowania zaszyfrowanego dokumentu, pliku,
3) nieautoryzowany dostęp do bazy danych,
4) nieautoryzowane modyfikacje lub niszczenie danych,
5) nielegalne ujawnienie danych,
6) pozyskiwanie danych z nielegalnych źródeł,
7) ujawnienie wirusów komputerowych lub innych programów godzących w integralność systemu informatycznego,
8) kradzież sprzętu komputerowego lub nośników zawierających oprogramowanie lub dane,
9) wydarzenia losowe obniżające stan bezpieczeństwa systemu (brak zasilania, pożar, itp.).

3. Sytuacje wskazujące na naruszenie zabezpieczenia danych osobowych

Sytuacjami, które mogą wskazywać, że zostały naruszone zabezpieczenia danych osobowych mogą być takie sytuacje, które odbiegają od przyjętych procedur i standardów, a zwłaszcza:

1) naruszenie zasad wynikających z Polityki Bezpieczeństwa Przetwarzania Danych Osobowych,
2) naruszenie (uszkodzenie) zabezpieczeń technicznych (fizycznych) w pomieszczeniach (wyłamane zamki, naruszone plomby, ujawnione próby manipulowania przy zamkach itp.), w tym potwierdzone przez organy ścigania włamania i kradzieże,
3) ujawnienie faktu manipulowania urządzeniami i systemami zabezpieczającymi dostęp do bazy danych,
4) anomalie w pracy systemu lub programu,
5) ujawnienie haseł dostępu do systemu informatycznego,
6) notowanie w krótkim czasie dużej liczby nieudanych prób logowania,
7) korzystanie z zasobów systemu poza zgłoszonymi godzinami pracy,

Szkoła Podstawowa w Lechowie
Lechów 66, 26-004 Bieliny
tel. 413025369

8) zmiana lub utrata danych zapisanych na kopiach zapasowych lub archiwalnych, dokonana w sposób nieautoryzowany,
9) stwierdzenie nadmiernych, w stosunku do wykonywanych zadań, uprawnień użytkownika do zasobów systemu,
10) nieuprawnione wykonanie kserokopii dokumentu zawierającego dane osobowe,
11) omyłkowe wyniesienie na zewnątrz dokumentów lub nośników zawierających dane osobowe, przez osobę nieuprawnioną,
12) przesłanie przy użyciu sieci publicznej wiadomości e-mail zawierającej dane osobowe, bez żadnego zabezpieczenia tych danych.

4. Przedmiot instrukcji

Przedmiotem instrukcji są zasady postępowania wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych, a także innych osób uprawnionych do dostępu i/lub przetwarzania danych osobowych.

5. Procedura zgłoszenia naruszenia

1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub gdy zaistniała sytuacja, która mogłaby wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych lub inna osoba uprawniona do przetwarzania danych osobowych, niezwłocznie przerywa przetwarzanie danych osobowych i zawiadamia o tym zdarzeniu ADO.
2. Zgłoszenia faktu naruszenia ochrony danych osobowych należy dokonać niezwłocznie, osobiście lub telefonicznie, a następnie w ciągu 2 godzin od zgłoszenia zaistnienia zdarzenia, określonego w punkcie 1, należy opisać powstały incydent wypełniając dokument „Zgłoszenie naruszenia ochrony danych osobowych", **którego wzór stanowi załącznik nr 1 do niniejszej instrukcji.**

6. Podjęcie działań naprawczych

1. ADO, po powzięciu informacji o zdarzeniu, informuje IOD i wraz z nim podejmuje działania naprawcze, mające na celu:
   1) minimalizację skutków zdarzenia, w tym doprowadzenie do sytuacji uniemożliwiającej dalsze bezprawne przetwarzanie danych osobowych,
   2) zabezpieczenie dowodów zdarzenia,
   3) wyjaśnienie okoliczności zdarzenia,
   4) zgłoszenie naruszenia organowi nadzorczemu, zgodnie z rozdziałem 7 instrukcji,
   5) zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, zgodnie z rozdziałem 8 instrukcji.
2. W celu realizacji zadań wynikających z niniejszej instrukcji ADO i IOD, lub inna upoważniona przez ADO osoba, ma prawo podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:
   1) żądania wyjaśnień od pracowników,
   2) korzystania z pomocy konsultantów,
   3) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.
3. Polecenia ADO, IOD lub innej upoważnionej przez ADO osoby, w ramach realizacji zadań wynikających z niniejszej instrukcji, są priorytetowe i winny być wykonane przed innymi.
4. Odmowa udzielenia wyjaśnień lub współpracy z podmiotami wskazanymi w punkcie 3 lub z UODO traktowana będzie jako naruszenie obowiązków pracowniczych.

7. Zgłoszenie naruszenia organowi nadzorczemu

Szkoła Podstawowa w Lechowie
Lechów 66, 26-004 Bieliny
tel. 413025369

1. W przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin od stwierdzenia naruszenia - zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Jeżeli w jakimś zakresie informacji nie da się udzielić niezwłocznie, można je udzielać sukcesywnie bez zbędnej zwłoki.
2. Zgłoszenie, o którym mowa w punkcie 1, musi co najmniej:
   a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
   b) zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
   c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
   d) opisywać środki zastosowane lub proponowane przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Organem właściwym do zgłoszenia naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO). Zgłoszenia należy dokonać za pomocą formularza dostępnego na stronie uodo.gov.pl.
4. Podmiot przetwarzający, po stwierdzeniu naruszenia ochrony danych osobowych, oprócz obowiązków, które nakładają na niego przepisy prawa, w tym obowiązku zgłoszenia naruszenia organowi nadzorczemu, również bez zbędnej zwłoki zgłasza ten fakt ADO.

8. Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w punkcie 1, ma opisywać charakter naruszenia ochrony danych osobowych oraz zawierać informacje i środki, o których mowa w rozdziale 7 punkt 2 b, c i d.
3. Zawiadomienie, o którym mowa w punkcie 1, nie jest wymagane, w następujących przypadkach:
   a) gdy, ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
   b) ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w punkcie 1,
   c) wymagałoby ono niewspółmiernie dużego wysiłku; w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

9. Czynności profilaktyczne

1. Jeżeli w wyniku przeprowadzenia procedury zgłoszenia naruszenia ADO stwierdzi, że istniała możliwość naruszenia ochrony danych osobowych, ale do naruszenia nie doszło, ADO, przy udziale IOD przeprowadza czynności profilaktyczne, mające za zadanie zwiększenie zabezpieczenia chronionych i przetwarzanych danych osobowych, polegające m.in. na:
   a) wprowadzeniu dodatkowych środków organizacyjnych (np. poprzez wprowadzenie nowej lub uszczegółowienie dotychczasowej Polityki lub innej wewnętrznej procedury),

Szkoła Podstawowa w Lechowie
Lechów 66, 26-004 Bieliny
tel. 413025369

b) wymianie dotychczasowych (lub wprowadzeniu dodatkowych) zabezpieczeń fizycznych (np. wymiana zamka, założenie kłódki, zamocowanie krat lub rolet antywłamaniowych),
c) wzmocnieniu zabezpieczenia systemu komputerowego (np. zwiększenie częstotliwości zmiany haseł dostępu, zainstalowanie nowszej aplikacji antywirusowej).

2. Incydent, który nie skutkuje naruszeniem danych osobowych należy udokumentować w protokole, **którego wzór stanowi załącznik nr 2.**
3. Opisane w punkcie 1 czynności profilaktyczne ADO wdraża również w sytuacji, gdy do naruszenia ochrony danych osobowych doszło, wprowadzono działania naprawcze i całkowicie zniwelowano stan naruszenia i zagrożenia. Czynności te, w tym przypadku, mają służyć zwiększeniu bezpieczeństwa chronionych danych.

10. Rejestr incydentów

1. Dokumentuje się wszelkie incydenty i naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania naprawcze i czynności profilaktyczne, w formie rejestru.
2. Rejestr naruszeń i incydentów może posłużyć również UODO, przy wykonywaniu czynności merytorycznych, w tym zaradczych oraz kontrolnych.
3. Rejestr naruszeń i incydentów prowadzi IOD, **według wzoru z załącznika nr 3.**

11. Sankcje

1. Nie przestrzeganie zasad postępowania określonych w niniejszej instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej, wynikającej z Regulaminu pracy, a także określonej w art. 52 i art. 108 Kodeksu Pracy.
2. Jeżeli skutkiem działania określonego w punkcie 1 jest ujawnienie informacji osobie nieuprawnionej, sprawca może być pociągnięty do odpowiedzialności karnej wynikającej z Kodeksu Karnego.
3. Jeżeli skutkiem działania określonego w punkcie 1 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz prawa cywilnego.

Szkoła Podstawowa w Lechowie
Lechów 66, 26-004 Bieliny
tel. 413025369

Zgłoszenie naruszenia ochrony danych osobowych

Administrator Danych Osobowych
……
……
……

1. Data: …… Godzina: ……
(dd.mm.rr) (gg:mm)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

……
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:

……
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

……

……

……

……
(data, podpis osoby zgłaszającej)

Szkoła Podstawowa w Lechowie
Lechów 66, 26-004 Bieliny
tel. 413025369

PROTOKÓŁ INCYDENTU NARUSZENIA DANYCH OSOBOWYCH

Data i godzina wystąpienia incydentu:……..

Opis incydentu	
Przyczyny powstania incydentu	
Zaistniałe skutki incydentu	
Podjęte działania naprawczo-zapobiegawcze	

Inspektor Ochrony Danych

……..

Administrator Danych Osobowych

……..

Otrzymują:
1 x Administrator Danych Osobowych
1 x Inspektor Ochrony Danych

Szkoła Podstawowa w Lechowie
Lechów 66, 26-004 Bieliny
tel. 413025369

Wzór ewidencji naruszeń i incydentów naruszenia danych osobowych

L.p.	Data i godzina naruszenia /incydentu	Rodzaj naruszenia /incydentu	Opis naruszenia /incydentu	Skutki naruszenia /incydentu	Działania naprawcze	Podpis IOD

Szkoła Podstawowa w Lechowie
Lechów 66, 26-004 Bieliny
tel. 413025369