Załącznik nr 3 do Zarządzenia nr 12/2018
dyrektora Szkoły Podstawowej im. Jana Pawła II w Chwarstnicy
z dnia 03.09.2018r.

Instrukcja Postępowania w Sytuacji Naruszeń podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej

w Szkole Podstawowej im. Jana Pawła II w Chwarstnicy

ul. Gryfińska 19, 74-100 Gryfino

Szczegóły dokumentu:

Sporządził:	*Marta Maj* Inspektor Ochrony Danych
Data przekazania:	01.09.2018r.

Historia zmian

Data	Wersja	Utworzona przez	Opis zmiany

Spis treści

1. *Istota naruszenia bezpieczeństwa informacji.*

Zagrożenia losowe wewnętrzne w szczególności niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania - może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.

Zagrożenia losowe zewnętrzne w szczególności klęski żywiołowe, przerwy w zasilaniu - ich występowanie może prowadzić do utraty integralności danych ich zniszczenia i uszkodzenia infrastruktury technicznej systemu.

Zagrożenia zamierzone, świadome i celowe, naruszenia poufności danych, możemy podzielić na:

a) nieuprawniony dostęp do systemu z zewnątrz,
b) nieuprawniony przekaz danych,
c) nieuprawniony dostęp do systemu z jego wnętrza,
d) pogorszenie jakości sprzętu i oprogramowania.

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to w szczególności:

a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej, itp.,
b) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych, a także niewłaściwe działanie serwisu,
c) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
d) stwierdzenie próby lub modyfikacji danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
e) wystąpienie niedopuszczalnej manipulacji danymi osobowymi w systemie,
f) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur,
g) ujawnienie, istnienie nieautoryzowanych kont dostępu do danych,
h) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowanie lub skopiowanie danych osobowych,
i) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały,) na nośnikach tradycyjnych tj. na papierze (wydrukach), zdjęciach, płytach w formie niezabezpieczonej itp.

2. *Podstawowe pojęcia i skróty.*

Słownik podstawowych pojęć oraz skrótów występujących w niniejszej instrukcji znajduje się w dokumencie Polityki Bezpieczeństwa Informacji.

3. *Postępowanie w przypadku naruszenia bezpieczeństwa informacji*

Każdy pracownik biorący udział w przetwarzaniu danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób) jest odpowiedzialny za bezpieczeństwo tych danych.

Każda osoba zatrudniona, która zauważyła zdarzenie, które może być przyczyną naruszenia ochrony danych osobowych lub może spowodować naruszenie bezpieczeństwa danych, **zobowiązana jest do natychmiastowego poinformowania Administratora Danych.**

Informacja o pojawieniu się zagrożenia danych osobowych powinna być przekazywana przez pracownika osobiście, telefonicznie lub pocztą elektroniczną. Powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia.

Każdy pracownik, który stwierdzi fakt naruszenia bezpieczeństwa ma obowiązek:

a) zabezpieczyć dostęp do miejsca lub urządzenia przez osoby trzecie,
b) wstrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiać bez koniecznej potrzeby komputerów i innych urządzeń, których funkcjonowanie w związku naruszeniem ochrony zostało wstrzymane,
c) podjąć stosownie do zaistniałej sytuacji działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
d) powinien udokumentować zaistniałe naruszenie.

Administrator Danych niezwłocznie po uzyskaniu sygnału o naruszeniu danych osobowych, powinien:

a) zapisać informacje związane z danym zdarzeniem,
b) nawiązać kontakt ze specjalistami jeżeli zachodzi taka potrzeba,
c) zidentyfikować rodzaj zdarzenia,
d) zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
e) poinformować o naruszeniu bezpieczeństwa danych osobowych Organ Nadzorczy oraz osoby, których dane są przetwarzane, a bezpieczeństwo zostało naruszone, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

System informatyczny, którego prawidłowe działanie zostało odtworzone, powinien zostać poddany szczegółowej obserwacji. W czasie jej trwania użytkowanie systemu informatycznego powinno być ograniczone do niezbędnego minimum.

4. Sankcje karne

Wobec osoby, która w przypadku naruszenia bezpieczeństwa informacji nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.

Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu bezpieczeństwa informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z innymi regulacjami prawnymi.

5. Podstawy prawne.

Podstawy prawne niniejszej ISPN znajdują się w dokumencie Polityki Bezpieczeństwa Informacji.

6. Postanowienia końcowe.

W sprawach nieuregulowanych niniejszą ISPN odpowiednie zastosowanie mają reguły i procedury zawarte w dokumentach powiązanych.

Instrukcja Postępowania w Sytuacji Naruszeń w Szkole Podstawowej w Chwarstnicy wchodzi

w życie z dniem podpisania.

……

(podpis Administratora Danych)