Załącznik nr 3

do Zarządzenia nr 23 2017/2018

Dyrektora Publicznej Szkoły Podstawowej nr 1

im. Klaudyny Potockiej w Pułtusku

z dnia 27.04.2018r.

w sprawie wprowadzenia

„Polityki ochrony danych osobowych"

w Publicznej Szkole Podstawowej nr 1 im. Klaudyny Potockiej w Pułtusku

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA SYSTEMU OCHRONY DANYCH OSOBOWYCH

w

Publicznej Szkole Podstawowej nr 1 im. Klaudyny Potockiej w Pułtusku

Rozdział 1

Postanowienia ogólne

§ 1

1. Instrukcja niniejsza określa tryb i zasady postępowania osób zatrudnionych przy przetwarzaniu danych osobowych, w przypadku gdy:

   1) stwierdzenia naruszenia złamania zabezpieczeń technicznych, organizacyjnych i osobowej zbiorów danych osobowych,

   2) stwierdzono naruszenie zabezpieczenia systemu informatycznego,

   2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń danych.

2. Osobą odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań

w przypadku wykrycia naruszeń w systemie, jest wyznaczony przez administratora inspektor ochrony danych osobowych i jego zastępca.

Rozdział 2

Symptomy naruszenie sytemu bezpieczeństwa przetwarzanych zbiorów

§ 2

1. Użytkownik jest zobowiązany niezwłocznie powiadomić administratora, inspektora ochrony danych osobowych lub jego zastępcę, jeśli stwierdzi, że doszło do naruszenia ochrony danych osobowych lub będzie miał podejrzenie, że mogło dojść do takiego zdarzenia.
2. **Typowe sytuacje, o których użytkownik powinien powiadomić inspektora ochrony danych:**
   1) ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
   2) ujawniona kradzież aktywów,
   3) zniszczenie dokumentacji zawierającej dane osobowe bez użycia niszczarki,
   4) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
   5) otwarte drzwi do pomieszczeń, szaf, w których przechowywane są dane osobowe,
   6) ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
   7) wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz firmy bez upoważnienia inspektora ochrony danych,
   8) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
   9) telefoniczne próby wyłudzenia danych osobowych,
   10) kradzież komputerów lub CD, twardych dysków, pendrive'a z danymi osobowymi,
   11) e-maile zachęcające do ujawnienia identyfikatora i/lub hasła,
   12) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
   13) przechowywanie haseł do systemów w pobliżu komputera.

Rozdział 3

Tryb i zasady postępowania w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego

§ 3

1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego osoba stwierdzająca naruszenie obowiązana jest niezwłocznie powiadomić o tym administratora

bezpieczeństwa informacji.

2. Administrator i inspektor ochrony danych osobowych po otrzymaniu powiadomienia:

   1) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu (odłączenie urządzeń, zmiana haseł),

   2) zabezpiecza, utrwala wszelkie informacje i dokumenty, które mogą stanowić pomoc przy ustaleniu przyczyn naruszenia,

   3) ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,

   4) niezwłocznie przywraca prawidłowy stan działania systemu, a w przypadku uszkodzenia baz danych odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności,

   5) dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,

   6) sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu (włamaniu do systemu), opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia,

   7) w przypadku incydentu prowadzone jest komisyjne wewnętrzne postepowania wyjaśniające pod przewodnictwem inspektora ochrony danych osobowych,

   7) **w przypadku rażącego naruszenia systemu bezpieczeństwa** ochrony danych administrator lub działający w jego imieniu inspektor ochrony danych osobowych zgłasza do Urzędu Ochrony Danych Osobowych w ciągu **72 godzin**, a jeżeli naruszenie ma znamiona przestępstwa także prokuraturę.

3. Raport wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie) inspektor ochrony danych osobowych przekazuje administratorowi.
4. Inspektor ochrony danych osobowych w porozumieniu z administratorem podejmuje niezbędne działania w celu zapobieżenia naruszeniom zabezpieczeń systemu w przyszłości.

Rozdział 4

Tryb postępowania w przypadku podejrzenia naruszenia zabezpieczeń danych osobowych

§ 4

1. **Każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczeń danych osobowych, obowiązana jest niezwłocznie powiadomić o tym inspektora ochrony danych osobowych, administratora lub inną upoważnioną przez niego osobę.**
2. **Inspektor ochrony danych osobowych po otrzymaniu powiadomienia (stosownie do przypuszczalnego rodzaju naruszeń):**
   1) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
   2) sprawdza sposób działania programu (w tym również obecność wirusów komputerowych),
   3) sprawdza jakość komunikacji w sieci telekomunikacyjnej,
   4) sprawdza zawartość zbioru danych osobowych,
   5) poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych.
3. **W przypadku stwierdzenia naruszenia zabezpieczeń danych:**
   1) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia (odłączenie wadliwych urządzeń, blokuje dostęp do sieci telekomunikacyjnej, do programów oraz zbiorów danych itp.),
   2) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,
   3) niezwłocznie przywraca prawidłowy stan działania systemu,
   4) dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek ich naruszenia,
   5) sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.
4. Raport, wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie), inspektor ochrony danych osobowych przekazuje administratorowi danych osobowych

jednostki.

5. Inspektor ochrony danych osobowych, w porozumieniu z administratorem, podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:

    1) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza, w stosownym zakresie, przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,

    2) jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje do administratora danych osobowych o wyciągniecie konsekwencji prawem przewidzianych.

Rozdział 5

Postanowienia końcowe

§ 5

1. Każda osoba wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych zobowiązana jest do zapoznania się z niniejszą instrukcją.
2. Wykonanie powyższego zobowiązania pracownik potwierdza własnoręcznym podpisem.
3. Wszelkie zmiany niniejszej instrukcji wchodzą w życie wobec osób, których dotyczą, z datą ich zapisania.