że doszło do naruszenia przepisów o ochronie danych osobowych.

2.6. ODPOWIEDZIALNOŚĆ PRACOWNIKÓW I UŻYTKOWNIKÓW SYSTEMU

1. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest zaangażowanie ze strony każdego pracownika w zakresie ochrony danych osobowych.
2. Pracownicy Szkoły są zobowiązani do informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe bezpośrednio do Administratora Bezpieczeństwa Informacji.
3. Pracownicy są zobowiązani w szczególności do:
   a. postępowania zgodnie z Polityką i wszelkimi regulaminami, procedurami z nią związanymi;
   b. zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia;
   c. ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
   d. wykonywania konkretnych działań i procesów w celu zapewnienia ochrony danych osobowych.
4. Pracownicy powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych. W tym celu powinni przestrzegać zasad określonych w sposobie postępowanie w razie naruszenia bezpieczeństwa ochrony danych osobowych opisanych w niniejszej polityce (patrz tabele 1-3).
5. Pracownicy powinni na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać IODprojekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu ochrony danych osobowych.

3. ZAGROŻENIA BEZPIECZEŃSTWA

1.1. CHARAKTERYSTYKA MOŻLIWYCH ZAGROŻEŃ

Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, nagłe przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, a ciągłość systemu zostaje zakłócona lecz nie dochodzi do naruszenia poufności danych.
Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki użytkowników, administratora systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia danych, a ciągłość pracy systemu może zostać zakłócona oraz może nastąpić naruszenie poufności danych,
Zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, gdzie występuje naruszenie poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na:

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

1.2. SYTUACJE ŚWIADCZĄCE O NARUSZENIU ZASAD BEZPIECZEŃSTWA

Przełamane zabezpieczeń tradycyjnych –wyłamane zamki w drzwiach, szafach, wybite okna.
Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
Niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
Naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
Próba lub modyfikacja danych oraz zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
Niedopuszczalna manipulacja danymi osobowymi w systemie,