INSTRUKCJA ALARMOWA W PRZYCHODNI MEDYCYNY RODZINNEJ VIOLETTA ŻYLIŃSKA

Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych zobowiązany jest poinformować bezpośredniego przełożonego lub inspektora ochrony danych.

2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

    1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
    2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
    3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

3. Do typowych incydentów bezpieczeństwa danych osobowych należą:

    1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
    2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych);
    3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. W przypadku stwierdzenia zagrożenia bezpieczeństwa danych osobowych inspektor ochrony danych prowadzi postępowanie wyjaśniające, w toku którego:

    1) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;
    2) inicjuje ewentualne działania dyscyplinarne;
    3) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
    4) dokumentuje prowadzone postępowania.

5. W przypadku stwierdzenia incydentu (naruszenia) bezpieczeństwa danych osobowych inspektor ochrony danych prowadzi postępowanie wyjaśniające, w toku którego:

    1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;
    2) zabezpiecza ewentualne dowody;
    3) ustala osoby odpowiedzialne za naruszenie;
    4) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
    5) inicjuje działania dyscyplinarne;
    6) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;
    7) dokumentuje prowadzone postępowania.

Opracował:

/-/ Marek Pakuła

Inspektor Ochrony Danych