


ZATWIERDZAM

mgr inż. Dariusz Gil

 01.10.2019 r.
mgr inż. Dariusz Gil

(data, pieczęć imienna, podpis)

Instrukcja alarmowa

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.

Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych zobowiązany jest poinformować bezpośredniego przełożonego lub Pełnomocnika Ochrony Danych.

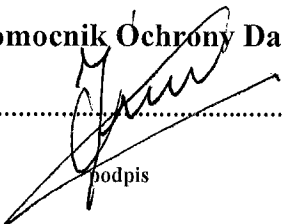
1. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
 - a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
 - b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
 - c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

2. Do typowych incydentów bezpieczeństwa danych osobowych należą:
 - a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
 - b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
 - c. 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).

3. W przypadku stwierdzenia wystąpienia zagrożenia oraz incydentu (naruszenia) Administrator Danych Osobowych prowadzi postępowanie wyjaśniające, w toku którego:
 - a. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
 - b. inicjuje ewentualne działania dyscyplinarne,

- c. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
- d. dokumentuje prowadzone postępowania,
- e. ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
- f. zabezpiecza ewentualne dowody,
- g. ustala osoby odpowiedzialne za naruszenie,
- h. podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
- i. inicjuje działania dyscyplinarne,
- j. wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
- k. dokumentuje prowadzone postępowania.

Pełnomocnik Ochrony Danych

.....

podpis

