INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

§1 Postanowienia ogólne

1. Instrukcja niniejsza określa tryb i zasady postępowania osób zatrudnionych przy przetwarzaniu danych osobowych w przypadku, gdy:
a) stwierdzi się naruszenie zabezpieczeń systemu informatycznego,
b) 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 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 **Administrator Danych Osobowych**.

§2 Sytuacje naruszenia ochrony danych osobowych

1. Za naruszenie ochrony systemu informatycznego uważa się:
a) naruszenie lub próbę naruszenia integralności systemu oraz zbioru danych,
b) nieuprawniony dostęp, próbę dostępu do systemu lub pomieszczeń (widoczne uszkodzenia albo naruszenia zabezpieczeń),
c) nieautoryzowane zniszczenie lub próbę zniszczenia danych zgromadzonych w systemie,
d) zmianę lub utratę danych zapisanych na kopiach zapasowych lub archiwalnych dokonaną w sposób nieautoryzowany,
e) nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
f) inny stan systemu lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu lub po przerwie w pracy z systemem.

2. Instrukcję stosuje się odpowiednio w przypadku stwierdzenia, że stan pomieszczeń i szaf albo innych mebli biurowych, w których przechowywana jest dokumentacja lub zawartości tej dokumentacji wzbudzają podejrzenie, że dostęp do nich mogły mieć osoby nieupoważnione.

§3 Przedsięwzięcia organizacyjne zabezpieczające przed naruszeniem systemu ochrony danych osobowych

1. Do pomieszczeń, w których przetwarza się dane osobowe, powinny mieć stały dostęp tylko **osoby upoważnione przez Pracodawcę**.

2. Klucze do pomieszczeń, w których przetwarza się dane, po godzinach pracy muszą być przechowywane u ochrony budynku. Sposób ich wydawania i ochrony określają **odrębne uregulowania**.

3. Klucze zapasowe przechowuje się w zapieczętowanej kopercie w specjalnej szafie.

4. Dokonuje się regularnych kontroli, oceny funkcjonowania mechanizmów zabezpieczeń i ochrony w danym wydziale.

§4 Postępowanie w przypadku stwierdzenia lub podejrzenia naruszeń zabezpieczeń systemu informatycznego przetwarzającego dane osobowe.

1. W przypadku stwierdzenia naruszenia lub wystąpienia okoliczności wskazujących na naruszenie zabezpieczeń systemu informatycznego, w którym przetwarzane są dane osobowe, użytkownik systemu zobowiązany jest do bezzwłocznego powiadomienia o tym **Administratora Danych Osobowych.**

2. Użytkownik niezwłocznie:
a) zabezpiecza dostęp do miejsca lub urządzenia przez osoby nieupoważnione,
b) wstrzymuje pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, które w związku z naruszeniem ochrony zostały wstrzymane,
c) podejmuje, stosownie do zaistniałej sytuacji, inne, niezbędne działania w celu zapobiegnięcia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

3. Administrator Danych Osobowych po przybyciu na miejsce, w którym doszło do naruszenia ochrony danych osobowych:
a) ocenia sytuację, biorąc pod uwagę stan pomieszczeń, w których przetwarzane są dane, stan urządzeń i zbioru danych oraz identyfikuje wielkość negatywnych następstw naruszenia ochrony danych osobowych,
b) podejmuje działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu (odłączenie urządzeń, odłączenie wadliwych urządzeń, zmianę haseł, zablokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych),
c) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia, jak również sprawdza zawartość zbioru danych osobowych,
d) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
e) sprawdza sposób działania programu (**w tym również obecność wirusów komputerowych**),
f) ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,
g) zapewnia przywrócenie prawidłowego stanu działania systemu, a w przypadku uszkodzenia baz danych, odtwarza je z ostatnich kopii awaryjnych z zachowaniem środków ostrożności,
h) sprawdza jakość komunikacji w sieci telekomunikacyjnej,
i) dokonuje analizy stanu systemu z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia oraz poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych.

4. Zgodę na uruchomienie komputerów, innych urządzeń oraz kontynuowanie pracy wyraża Administrator Danych Osobowych zarządzający sieciami i systemami informatycznymi.

5. Dokonywanie zmian w miejscu naruszenia ochrony danych bez uzyskania zgody, o której mowa w **ust. 4** jest dopuszczalne, jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobiegnięcia grożącemu niebezpieczeństwu.

6. Administrator Danych Osobowych podejmuje działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, w szczególności:
a) 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,
b) 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 o wyciągnięcie

konsekwencji służbowych lub innych przewidzianych przepisami.