**Załącznik Nr 1**
**do Procedury postępowania**
**z naruszeniem ochrony danych osobowych**

PRZYKŁADOWY KATALOG NARUSZEŃ ZAGRAŻAJĄCYCH BEZPIECZEŃSTWU DANYCH OSOBOWYCH

**1.Formy naruszenia bezpieczeństwa danych osobowych przez pracownika zatrudnionego przy przetwarzaniu danych:**

- w zakresie wiedzy:
1) Ujawnienie sposobu działania aplikacji i systemu oraz jej zabezpieczeń,
2) Ujawnienie informacji o sprzęcie i pozostałej infrastrukturze informatycznej,
3) Dopuszczenie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać, np. z obserwacji lub dokumentacji,

- w zakresie sprzętu i oprogramowania:
1) Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych,
2) Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony,
3) Ujawnienie haseł dostępu lub pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci,
4) Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osoby nieuprawnione,
5) Samodzielne instalowanie jakiegokolwiek oprogramowania,
6) Modyfikowanie parametrów systemu i aplikacji,
7) Odczytywanie nośników danych przed sprawdzeniem ich programem antywirusowym,
8) Utrata komputera lub innego nośnika danych (np. telefon, tablet, USB),

- w zakresie dokumentów i obrazów zawierających dane osobowe:
1) Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru,
2) Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych,
3) Nieodpowiednie wyrzucanie dokumentów zawierających dane osobowe,
4) Dopuszczenie do nadmiernego kopiowania dokumentacji i utraty kontroli nad kopią,
5) Dopuszczenie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe,
6) Sporządzanie kopii danych na nośnikach i „wynoszenie” poza obszar ochrony danych bez zgody i wiedzy administratora,
7) Utrata kontroli nad kopią danych osobowych,
8) Utrata teczki zawierające dane w wersji papierowej,

 - w zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych:
1) Umożliwienie osobom nieuprawnionym dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
2) Dopuszczenie, aby osoby spoza pracowników CI podłączały jakiekolwiek urządzenia do sieci komputerowej, domontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji,

- w zakresie pomieszczeń, w których znajdują się komputery centralne i urządzenia sieci:
1) Dopuszczenie lub ignorowanie faktu, że osoby spoza pracowników CI dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (korytarze itp.),
2) Umożliwienie osobom nieuprawnionym dostępu do pomieszczeń, w których znajdują się komputery centralne lub węzły sieci komputerowej,

- inne:
1) Zmiana danych bez zgody osoby, której dane dotyczą,
2) Wysłanie danych do niewłaściwej osoby (np. poprzez niewłaściwie zaadresowanie poczty elektronicznej),
3) Nieuprawnione udostępnienie danych (np. elektronicznie czy np. telefonicznie, kiedy to rozmówca podaje się np. za pracownika policji czy urzędu, próbując wyciągnąć informacje),
4) Nieodpowiednie usuwanie danych (np. administrator postanawia sprzedać stare komputery, a przed sprzedażą usuwa jedynie pliki na pulpicie i opróżnia kosz, nie usuwając danych z dysku komputera).

**2.Formy naruszenia bezpieczeństwa danych osobowych niezależne od działalności człowieka:**1) zdarzenia losowe, np. powódź, pożar, ulewny deszcz, bardzo wysokie temperatury, bardzo wysoka wilgotność itp.,
2) zdarzenia niezależne od działalności człowieka lub nią nie spowodowane, np. zużycie sprzętu, starzenie się nośników pamięci, zmiany napięcia w sieci, utrata prądu, zbieranie się ładunków elektrostatycznych, zakłócenia elektromagnetyczne, radiotechniczne, defekty oprogramowania.

**3. Okoliczności świadczące o możliwości naruszenia ochrony danych osobowych:**1) Ślady manipulacji przy układach sieci komputerowej lub komputerach,
2) Obecność nowych kabli o nieznanym przeznaczeniu lub pochodzeniu,
3) Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych,
4) Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych,
5) Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe,
6) Wykorzystano niezinwentaryzowany środek przetwarzania informacji (nie będący własnością pracodawcy),
7) Pojawienie się nieautoryzowanej informacji na stronie internetowej.