Załącznik Nr 13
do Polityki

TABELA FORM NARUSZEŃ
bezpieczeństwa danych osobowych
(katalog zagrożeń i incydentów)

instrukcja postępowania dla osób posiadających upoważnienie do przetwarzania danych osobowych

KOD NARUSZENIA	FORMA NARUSZENIA	
A	**Forma naruszenia ochrony danych osobowych przez pracownika zatrudnionego przy przetwarzaniu danych**	
A.1.	W ZAKRESIE WIEDZY	SPOSÓB POSTĘPOWANIA
A.1.1.	Ujawnianie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Powiadomić bezpośredniego przełożonego oraz IOD. Sporządzić raport z opisem, jaka informacja została ujawniona.
A.1.2.	Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Powiadomić bezpośredniego przełożonego i IOD. Sporządzić raport z opisem, jaka informacja została ujawniona.
A.1.3.	Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać informacje o sprzęcie i pozostałej infrastrukturze informatycznej np. z obserwacji lub dokumentacji.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić IOD.
A.2.	W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA	SPOSÓB POSTĘPOWANIA
A.2.1.	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Pouczyć osobę, która dopuściła się takiej sytuacji. Sporządzić raport.
A.2.2.	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Sporządzić raport.
A.2.3.	Pozostawienie w jakimkolwiek niezabezpieczonym a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych i sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić IOD. Sporządzić raport.
A.2.4.	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić IOD. Sporządzić raport.
A.2.5.	Instalowanie oprogramowania lub wykorzystanie nielegalnego oprogramowania oraz narzędzi do obchodzenia zabezpieczeń w systemach informatycznych.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Sporządzić raport.
A.2.6.	Modyfikowanie parametrów systemu i aplikacji. (Zmiana konfiguracji sprzętowej oraz progowej systemów oraz stacji roboczych przez niepowołane osoby).	Wezwać osobę popełniającą wymieniona czynność, aby jej zaniechała. Pouczyć osobę popełniającą wymienioną czynność, aby stosowała się do wymogów bezpieczeństwa. Wezwać informatyka w celu przywrócenia stanu pierwotnego. Sporządzić raport.
A.2.7.	Odczytywanie nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport.
A.2.8.	Wykorzystanie ogólnodostępnych serwisów pocztowych (np.wp.pl ; onet.pl, o2pl. w celach służbowych).	Wezwać osobę popełniającą czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy. Sporządzić raport. Powiadomić IOD.
A.2.9.	Wykorzystywanie służbowej poczty do celów prywatnych.	Wezwać osobę popełniającą czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy. Sporządzić raport. Powiadomić IOD.

A.3.	W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE	SPOSÓB POSTĘPOWANIA
A.3.1.	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Przyjąć wyjaśnienia od bezpośredniego przełożonego. Sporządzić raport.
A.3.2.	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń. Sporządzić raport.
A.3.3.	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
A.3.4.	Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport.
A.3.5.	Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane. Sporządzić raport.
A.3.6.	Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić IOD. Sporządzić raport
A.3.7.	Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić IOD. Sporządzić raport.
A.4.	W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	SPOSÓB POSTĘPOWANIA
A.4.1.	Opuszczanie i pozostawianie bez dozoru niezamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć (zamknąć) pomieszczenie. Powiadomić przełożonych. Sporządzić raport.
A.4.2.	Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić przełożonych i IOD. Sporządzić raport.
A.4.3.	Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i IOD . Sporządzić raport. Powiadomić ADO.
A.4.4.	Pozostawienie otwartych okien, drzwi po zakończeniu pracy.	Zabezpieczyć(zamknąć) pomieszczenie. Sporządzić raport.
A.4.5.	Pożar, zalanie.	Podjąć próbę odzyskania dokumentacji i sprzętu. Powiadomić przełożonych, zespół informatyczny oraz IOD. Sporządzić raport. Powiadomić ADO.
A.4.6.	Nie przestrzeganie zasad czystego biurka oraz czystego ekranu.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Powiadomić IOD. Sporządzić raport.
A.4.7.	Pozostawienie dokumentacji w koszu na śmieci.	Zabezpieczyć dokumentację. Przekazać informacje do IOD. Sporządzić raport.
A.4.8.	Pozostawienie dokumentacji lub wydruków na ogólnodostępnej drukarce.	Zabezpieczyć dokumentację. Przekazać informacje do IOD. Sporządzić raport.
A.4.9.	Samowolne wykonanie kopii klucza do pomieszczenia biurowego.	Wezwać osobę pełniącą wymienioną czynność, aby jej zaniechała. Powiadomić IOD. Sporządzić raport.
A.4.10.	Wyniesienie kluczy od pomieszczenia biurowego po zakończeniu pracy.	Wezwać osobę pełniącą wymienioną czynność, aby jej zaniechała. Powiadomić IOD. Sporządzić raport.
A.4.11.	Próba kradzieży danych osobowych w formie papierowej.	Należy nie dopuścić do kradzieży danych, zabezpieczyć nośnik i powiadomić IOD. Sporządzić raport. Powiadomić ADO.
A.4.12.	Nieuprawniony dostęp do danych osobowych w formie papierowej.	Należy nie dopuścić do kradzieży danych, zabezpieczyć nośnik i powiadomić IOD. Sporządzić raport.
A.5.	W ZAKRESIE POMIESZCZEŃ W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI	SPOSÓB POSTĘPOWANIA
A.5.1.	Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i do opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i IOD. Sporządzić raport.
A.5.2.	Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i IOD. Sporządzić raport.

B	Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych	
B.1.	Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.2.	Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Służby informatyczne sporządzają raport, który przekazać należy do IOD.
B.3.	Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Służby informatyczne sporządzają raport, który przekazać należy do IOD.
B.4.	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Służby informatyczne sporządzają raport, który przekazać należy do IOD.
B.5.	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Służby informatyczne sporządzają raport, który przekazać należy do IOD.
B.6.	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie IOD. Sporządzić raport.
B.7.	Zidentyfikowano środek przetwarzający informacje nieznanego pochodzenia (sprzęt, nośnik).	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.8.	Przechowywanie haseł w niewłaściwy sposób.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Powiadomić IOD. Sporządzić raport.
B.9.	Przekazywanie haseł innym osobom.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Powiadomić IOD. Sporządzić raport.
B.10.	Niewłaściwe niszczenie nośników z danymi (możliwość ich odczytania).	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Powiadomić IOD. Sporządzić raport.
B.11.	Nieuprawniona zmiana danych lub ich uszkodzenie.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Powiadomić IOD. Sporządzić raport.
B.12.	Fizyczne zniszczenie lub uszkodzenie sprzętu komputerowego.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Służby informatyczne sporządzają raport, który przekazać należy do IOD.
B.13.	Kradzież sprzętu komputerowego.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Służby informatyczne sporządzają raport, który przekazać należy do IOD.
B.14.	W związku z rozwiązaniem umowy o pracę, nie podjęto działań związanych z odebraniem uprawnień.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Służby informatyczne sporządzają raport, który przekazać należy do IOD.
C	**Formy naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem**	
C.1.	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	Powiadomić niezwłocznie IOD. Sporządzić raport.
C.2.	Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	Powiadomić niezwłocznie IOD. Sporządzić raport.
C.3.	Nie wykonanie kopii zapasowych.	Powiadomić niezwłocznie IOD. Sporządzić raport.
C.4.	Nie zweryfikowanie możliwości odtworzenia danych z kopii zapasowych.	Powiadomić niezwłocznie IOD. Sporządzić raport.