TABELA FORM NARUSZENIA OCHRONY DANYCH OSOBOWYCH PRZEZ OSOBY ZATRUDNIONE PRZY PRZETWARZANIU DANYCH

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
W ZAKRESIE WIEDZY	
Ujawnianie sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić Administratora lub Pełnomocnika Ochrony Danych.
Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	
Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać, np. z obserwacji lub dokumentacji.	
W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA	
Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport o naruszeniu.
Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż ta, której został przydzielony identyfikator.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Sporządzić raport o naruszeniu.
Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić Administratora lub Pełnomocnika Ochrony Danych. Sporządzić raport o naruszeniu.
Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych osobom nieuprawnionym.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić, jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić Administratora lub Pełnomocnika Ochrony Danych. Sporządzić raport o naruszeniu.
Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę wykonującą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Sporządzić raport o naruszeniu.
Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Sporządzić raport o naruszeniu.
Odczytywanie nośników CD/DVD, pendrive przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność o szkodliwości takiego działania. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport o naruszeniu.
W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE	
Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Sporządzić raport o naruszeniu.
Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń. Sporządzić raport o naruszeniu.
Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport o naruszeniu.
Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport o naruszeniu.
Dopuszczanie, aby inne osoby odczytywały dane osobowe wyświetlane na ekranie monitora.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane - sporządzić raport o naruszeniu.
Sporządzanie kopii danych na nośnikach danych w sytuacjach nieprzewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić administratora bezpieczeństwa

	informacji. Sporządzić raport.
Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić Administratora lub Pełnomocnika Ochrony Danych. Sporządzić raport o naruszeniu.
W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	
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 pomieszczenie. Powiadomić przełożonych. Sporządzić raport o naruszeniu.
Wpuszczanie do pomieszczeń osób nieznanych i przyzwalanie, by korzystały ze sprzętu komputerowego.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, ustalić ich tożsamość. Powiadomić Administratora lub Pełnomocnika Ochrony Danych. Sporządzić raport o naruszeniu.
Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiekolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub manipulowały przy nich.	Wezwać osoby wykonujące zakazane czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić Administratora lub Pełnomocnika Ochrony Danych. Sporządzić raport o naruszeniu.
W ZAKRESIE POMIESZCZEŃ, W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI	
Dopuszczenie, by osoby spoza służb informatycznych i telekomunikacyjnych manipulowały przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze itp.).	Wezwać osoby wykonujące zakazane czynności do ich zaprzestania i ewentualnie opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i Administratora lub Pełnomocnika Ochrony Danych. Sporządzić raport o naruszeniu.
Dopuszczanie do przebywania w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych.	Wezwać osoby wykonujące zakazane czynności do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i Administratora lub Pełnomocnika Ochrony Danych. Sporządzić raport o naruszeniu.