W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE	
Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Powiadomić IOD.
Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych.	Spowodować poprawienie zabezpieczeń. Powiadomić IOD.
Wyrzucanie dokumentów umożliwiających ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić IOD.
Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić IOD.
Dopuszczanie, aby osoby nieuprawnione 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 powiadomić IOD. Wezwać ASI w celu ustawienia wygaszacza ekranu.
Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Wezwać do zaprzestania kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić IOD.
W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	
Opuszczanie i pozostawianie bez dozoru otwartego 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.
Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby naruszające bezpieczeństwo do opuszczenia pomieszczeń, próbować ustalić ich tożsamość. Powiadomić przełożonych i administratora bezpieczeństwa informacji.
Dopuszczanie, aby osoby obce lub nieupoważnione podłączały jakiekolwiek urządzenia do sieci komputerowej, demontowały elementy obudowy sprzętu, gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby naruszające bezpieczeństwodo ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić IOD i ASI.
W ZAKRESIE POMIESZCZEŃ W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI	
Dopuszczenie lub ignorowanie faktu, że osoby nieuprawnione dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby naruszające bezpieczeństwo do zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić ASI i IOD.
Dopuszczanie do pomieszczeń, w których znajdują się komputery centralne lub węzły sieci komputerowej, osób innych niż ASI lub pracownicy telekomunikacyjni.	Wezwać osoby naruszające bezpieczeństwo do zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby ASI i IOD.

Tabela 2 – Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Powiadomić niezwłocznie IOD i ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.
Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Powiadomić niezwłocznie ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.
Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	