

Tabela form naruszeń bezpieczeństwa danych osobowych

Kod naruszenia	Formy naruszeń	Sposób postępowania
A	Forma naruszenia ochrony danych osobowych przez pracownika zatrudnionego przy przetwarzaniu danych	
A. 1	W zakresie wiedzy:	
A. 1. 1	Ujawnianie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić Administratora Bezpieczeństwa Informacji.
A. 1. 2	Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić Administratora Bezpieczeństwa Informacji.
A. 1. 3	Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić Administratora Bezpieczeństwa Informacji.
A. 2	W zakresie sprzętu i oprogramowania	
A. 2. 1	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport.
A. 2. 2	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiegokolwiek 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 Administratora Bezpieczeństwa Informacji. 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 Administratora Bezpieczeństwa Informacji. Sporządzić raport.
A. 2. 5	Samodzielne instalowanie jakiegokolwiek oprogramowania	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania

Załącznik nr 9

		programów. Sporządzić raport.
A. 2. 6	Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę pełniącą wymienioną czynność, aby jej zaniechała. Sporządzić raport.
A. 2. 7	Odczytywanie dyskiecików i innych nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę pełniącą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport.
A. 3	W zakresie dokumentów i obrazów zawierających dane osobowe	
A. 3. 1	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru	Zabezpieczyć dokumenty. 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 Administratora Bezpieczeństwa Informacji. Sporządzić raport.
A. 3. 7	Utrata kontroli nad kopią danych osobowych	Podjąć próbę odzyskania kopii. Powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.
A. 4	W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych	
A. 4. 1	Opuszczanie i pozostawianie bez dozoru nie zamkniętego 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 nieznanymi i dopuszczanie do ich kontaktu ze sprzętem	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich

Załącznik nr 9

	komputerowym	tożsamość. Powiadomić przełożonych i Administratora Bezpieczeństwa Informacji. 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 Administratora Bezpieczeństwa Informacji. Sporządzić raport.
A. 5	W zakresie pomieszczeń w których znajdują się komputery centralne i urządzenia sieci.	
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 czynności do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i Administratora Bezpieczeństwa Informacji. Sporządzić raport.
A. 5. 2	Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych lub ignorowania takiego faktu	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i Administratora Bezpieczeństwa Informacji. Sporządzić raport.
B	Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych	
B. 1	Ślady manipulacji przy układach sieci komputerowej lub komputerach	Powiadomić niezwłocznie Administratora Bezpieczeństwa Informacji 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. Sporządzić raport.
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. Sporządzić raport.
B. 4	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
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. Sporządzić raport.
B. 6	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie Administratora Bezpieczeństwa Informacji. Sporządzić raport.

Załącznik nr 9

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 Administratora Bezpieczeństwa Informacji. 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 Administratora Bezpieczeństwa Informacji. Sporządzić raport.