Wyższa Szkoła Menedżerska
w Warszawie

Instrukcja postępowania w sytuacji stwierdzenia przypadków naruszenia bezpieczeństwa informacyjnego w Wyższej Szkole Menedżerskiej w Warszawie

Załącznik nr 4 do zarządzenia Rektora WSM w Warszawie
nr 2/05/2018 z dnia 22 maja 2018 r.

Dokument przygotował: Dyrektor Centrum Administracyjno – technicznego inż. Dariusz Grabiec
Wersja dokumentu: 1/2018
Dokument zatwierdził: J.M. Rektor Prof. dr hab. Paweł Czarnecki MBA dr h.c.
Wprowadzono do stosowania Zarządzeniem Rektora nr 2/05/2018 w dniu: 22 maja 2018 r.

Spis treści

I. Wprowadzenie

1. Niniejsza Instrukcja jest aktem wykonawczym w odniesieniu do „Polityki Bezpieczeństwa Danych Osobowych". Wprowadza się ją w celu określenia na czym mogą polegać poszczególne rodzaje naruszeń bezpieczeństwa informacyjnego w Wyższej Szkole Menedżerskiej w Warszawie (WSM) i w jaki sposób oraz na jakiej podstawie zatrudnione w nim osoby powinny kwalifikować (rozpoznawać) określone zdarzenia jako potencjalne naruszenie bezpieczeństwa informacyjnego.
2. Celem Instrukcji jest określenie wymaganego sposobu postępowania wszystkich osób odpowiedzialnych za właściwe zabezpieczenie przetwarzanych w WSM danych, w szczególności Inspektora Ochrony Danych (IOD), w sytuacji gdy:
   - stwierdzono naruszenie zabezpieczenia systemu informacyjnego w obszarze przetwarzania danych,
   - stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie bezpieczeństwa danych,
   - stwierdzono naruszenie bezpieczeństwa fizycznego pomieszczeń, kartotek lub szaf, w których przechowywane są nośniki danych, w szczególności danych osobowych.
3. Instrukcja wprowadza również obowiązujące w WSM zasady dokumentowania zdarzeń dotyczących naruszenia bezpieczeństwa informacyjnego, a także procesu ich analizy pod kątem konieczności zgłoszenia faktu ich zaistnienia do Organu nadzorczego oraz osoby, której dane dotyczą.
4. Inspektor Ochrony Danych, we współpracy z Administratorem Systemu Informatycznego, podejmuje niezbędne działania zapewniające odporność sieci oraz systemów informatycznych na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne zjawiska naruszające dostępność, integralność i poufność przetwarzanych danych osobowych oraz bezpieczeństwo związanych z nimi usług oferowanych lub udostępnianych poprzez te sieci.
5. Każdy pracownik Uczelni biorący udział w przetwarzaniu danych osobowych jest odpowiedzialny za bezpieczeństwo tych danych. Na każdym pracowniku ciąży zarazem obowiązek zgłaszania do przełożonych lub bezpośrednio do IOD wszelkich stwierdzonych przez siebie naruszeń zasad bezpieczeństwa informacyjnego oraz zdarzeń mogących prowadzić do naruszenia bezpieczeństwa, w tym zwłaszcza zaobserwowanych podatności

na naruszenia. Informacja o pojawieniu się zagrożenia jest przekazywana przez pracownika osobiście, telefonicznie lub pocztą elektroniczną.

6. Dla stwierdzonych przypadków naruszenia zasad bezpieczeństwa danych osobowych należy zapewnić możliwość uzyskania danych niezbędnych do przeprowadzenia postępowania wyjaśniającego pod kątem określenia skutków naruszenia, ustalenia odpowiedzialności i sformułowania wniosków.

II. Definicje

W treści niniejszej Instrukcji zastosowanie mają definicje zawarte w rozdziale 1 Polityki Bezpieczeństwa Danych Osobowych PBDO), a także:

1. **Zdarzenie związane z bezpieczeństwem informacyjnym** – określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie PBDO, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacyjnym i prowadzić w konsekwencji do naruszenia ochrony danych osobowych;
2. **Incydent bezpieczeństwa** – pojedyncze zdarzenie lub seria niepożądanych oraz niespodziewanych zdarzeń związanych z bezpieczeństwem informacyjnym, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacyjnemu;
3. **Raport** – pisemny raport dot. naruszenia bezpieczeństwa informacyjnego;
4. **Rejestr** – Rejestr naruszeń bezpieczeństwa informacyjnego w Wyższej Szkole Menedżerskiej w Warszawie.

III. Rodzaje naruszeń bezpieczeństwa informacyjnego

1. Najbardziej typowe źródła zagrożeń bezpieczeństwa informacyjnego, szczególnie istotne z punktu widzenia przetwarzania danych osobowych, wyszczególniono w rozdziale 15 PBDO.
2. Dla potrzeb niniejszej Instrukcji wyróżnia się następujące główne rodzaje naruszeń bezpieczeństwa informacyjnego:
   a. naruszenie dostępności systemu informacyjnego;

b. naruszenie integralności systemu informacyjnego;
c. naruszenie poufności systemu informacyjnego.

3. Naruszenie dostępności systemu informacyjnego występuje wtedy, gdy użytkownik tego systemu nie jest w stanie wykonać autoryzowanej, zgodnej z dokumentacją funkcji użytkowej.
4. Naruszenie integralności systemu informacyjnego występuje wtedy, gdy postać lub treść danych (informacji) niezbędnych do wykonania legalnej funkcji użytkowej nie spełnia autoryzowanych wymagań lub, gdy wykonanie legalnej funkcji przebiega niezgodnie z autoryzowaną procedurą. Ten rodzaj naruszenia przejawiać się może również w przypadku dokonywania nieautoryzowanych modyfikacji lub niszczenia danych.
5. Naruszenie poufności systemu informacyjnego wystąpi wtedy, gdy dane (informacje) zostaną przypadkowo lub świadomie, udostępnione lub w inny sposób ujawnione nieautoryzowanym osobom, podmiotom lub procesom.
6. Niezależnie od określonych w przepisach ust. 3 – 5 rodzajów naruszeń, za naruszenie bezpieczeństwa informacyjnego w WSM uznane będzie również pozyskiwanie danych ze źródeł prawnie niedopuszczalnych.

IV. Zasady postępowania w przypadku naruszenia ochrony danych osobowych

1. Postępowanie w przypadkach naruszenia Polityki Bezpieczeństwa Danych Osobowych

   Każdy pracownik Uczelni biorący udział w przetwarzaniu danych osobowych jest odpowiedzialny za zapewnienie bezpieczeństwa tych danych. Na każdym pracowniku ciąży zarazem obowiązek zgłaszania do przełożonych lub bezpośrednio do IOD wszelkich stwierdzonych przez siebie naruszeń zasad bezpieczeństwa informacyjnego oraz zdarzeń mogących prowadzić do jego naruszenia, w szczególności zaobserwowanych podatności na naruszenia. Informacja o pojawieniu się zagrożenia jest przekazywana przez pracownika w sposób bezpośredni ustnie, drogą telefoniczną lub pocztą elektroniczną.

   Dla stwierdzonych przypadków naruszenia zasad bezpieczeństwa danych osobowych należy zapewnić możliwość uzyskania danych niezbędnych do przeprowadzenia postępowania wyjaśniającego pod kątem określenia skutków naruszenia, ustalenia odpowiedzialności i sformułowania wniosków.

2. Za symptomy wskazujące na potencjalną możliwość naruszenia bezpieczeństwa informacji, w tym bezpieczeństwa danych osobowych można uznać:
   - ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
   - wygląd aplikacji inny niż normalnie,
   - inny zakres danych niż normalnie dostępny dla użytkownika - dużo więcej lub dużo mniej danych,
   - znaczne spowolnienie działania systemu informatycznego,
   - pojawienie się niestandardowych komunikatów generowanych przez system informatyczny,
   - ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe,
   - ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii zapasowych,
   - włamanie lub próby włamania do szafek, w których przechowywane są, w postaci elektronicznej lub papierowej, nośniki danych osobowych,
   - zagubienie bądź kradzież nośnika danych osobowych,
   - kradzież sprzętu informatycznego, w którym przechowywane są dane osobowe,
   - fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia działania siły wyższej,
   - podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym,
   - podejrzenie, iż dane osobowe przetwarzane są w zakresie przekraczającym uzasadnioną potrzebę do realizacji określonego celu (nadmiarowość).

3. Zgłaszanie naruszenia (incydentu) ochrony danych osobowych Organowi nadzorczemu
   W przypadku wystąpienia incydentu, który może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki, w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza je Organowi

nadzorczemu. Do zgłoszenia przekazanego Organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Zgłoszenie każdorazowo musi być poprzedzone analizą ujawnionego incydentu, za przeprowadzenie której odpowiedzialny jest IOD we współpracy z ASI.

W zakres analizy incydentu bezpieczeństwa wchodzi realizacja co najmniej niżej wymienionych czynności:

- zabezpieczenie wszelkich znamion i dowodów związanych z zaistniałym incydentem,
- szczegółowy opis naruszenia, wskazujący w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- ocenę możliwych konsekwencji naruszenia praw lub wolności osób fizycznych;
- wyszczególnienie zastosowanych lub możliwych do zastosowania środków w celu zaradzenia lub choćby zminimalizowania ewentualnych skutków naruszenia.

Inspektor Ochrony Danych dokonuje wstępnej kwalifikacji każdego analizowanego przypadku, a następnie formułuje do Administratora (Rektora) wniosek w sprawie dokonania zgłoszenia do Organu nadzorczego lub odstąpienia od tej czynności w danym przypadku. Wniosek składany jest z całością zgromadzonego materiału w sprawie.

IOD w imieniu Administratora, dokumentuje i ewidencjonuje wszelkie naruszenia ochrony danych osobowych, z uwzględnieniem okoliczności każdego naruszenia, jego skutków oraz podjętych środków zaradczych. Dokumentacja ta musi pozwolić Organowi nadzorczemu na zweryfikowanie przestrzegania wymogów prawnych związanych z dokonywaniem zgłoszeń.

Za monitorowanie przestrzegania obowiązku zgłaszania naruszenia ochrony danych osobowych Organowi nadzorczemu odpowiedzialny jest Inspektor Ochrony Danych. Monitorowanie jest wynikiem stałej oceny ryzyka, prowadzonej przez IOD oraz stanowi również wynik innych analiz, w tym audytów bezpieczeństwa informacyjnego.

4. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu, chyba że wystąpią przypadki wskazane w prawie wyłączające konieczność zawiadomienia.

Za przejawy wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych można uznać w szczególności:

- przetwarzanie danych osobowych prowadzące do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych,
- przetwarzanie mogące skutkować dyskryminacją, kradzieżą tożsamości, lub oszustwem, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, znaczną szkodą gospodarczą lub społeczną,
- możliwość narażenia osoby, której dane dotyczą pozbawienia przysługujących jej praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi,
- przetwarzanie dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

Czynności związane z przeprowadzeniem pogłębionej analizy i kwalifikacji każdego tego rodzaju przypadku są realizowane zgodnie z zasadami określonymi w pkt. 3. Administrator, w przypadku stwierdzenia takiej konieczności, podejmuje inne niezbędne działania mające zapobiec materializacji negatywnych skutków związanych z naruszeniem praw osób, których to dotyczy.

V. Dokumentowanie naruszeń bezpieczeństwa informacyjnego

1. Najczęściej możliwe do zrealizowania się w Wyższej Szkole Menedżerskiej w Warszawie formy naruszeń bezpieczeństwa informacyjnego zamieszczono w tabeli, stanowiącej Załącznik nr 1 do niniejszej Instrukcji. Wykaz nie ma charakteru zamkniętego i w okresach nie krótszych niż pół roku podlega przeglądowi i aktualizacji, za przeprowadzenie której odpowiedzialny jest IOD.
2. Powzięcie przez uprawnionego użytkownika systemu informatycznego Wyższej Szkoły Menedżerskiej w Warszawie informacji o zaistniałym, bądź podejrzeniu zaistnienia Incydentu bezpieczeństwa, związanego w szczególności z naruszeniem przepisów dot. ochrony danych osobowych, nakłada na niego obowiązek powstrzymania się od dalszego przetwarzania tych danych i niezwłocznego powiadomienia osób wymienionych w rozdziale IV pkt. 1.
3. Po dokonaniu wstępnej analizy i kwalifikacji zaistniałego zdarzenia użytkownik jest obowiązany udokumentować ten fakt, poprzez sporządzenie Raportu, korzystając z wzoru

stanowiącego Załącznik nr 2 do niniejszej Instrukcji. Raport sporządzony w postaci elektronicznej bądź papierowej, jest następnie bez zbędnej zwłoki przekazywany do IOD, do którego należy podjęcie dalszych niezbędnych w tym zakresie czynności. Do czynności tych w szczególności zaliczyć można:

- zabezpieczenie dowodów zdarzenia,
- minimalizacja negatywnych skutków zdarzenia,
- wyjaśnienie wszelkich możliwych okoliczności zdarzenia.

4. W przypadku wystąpienia naruszenia bezpieczeństwa informacyjnego IOD wg własnej oceny może natychmiast powiadomić o takim zdarzeniu Rektora oraz podjąć dodatkowe działania związane ze sporządzeniem szczegółowej dokumentacji stwierdzonego naruszenia.
5. W sytuacji gdy naruszenie bezpieczeństwa informacyjnego związane jest z funkcjonowaniem systemu informatycznego, IOD współpracuje ściśle w tym zakresie z ASI. Wyniki ustaleń dokonanych przez ASI dokumentowane są w odrębnej notatce.
6. Dane zawarte w „Raporcie o naruszeniu bezpieczeństwa informacyjnego" oraz w treści notatki sporządzonej ewentualnie przez ASI, stanowią podstawę do dokonania wpisu w Rejestrze, wzór którego określono w Załączniku nr 3. Za prowadzenie Rejestru odpowiedzialny jest IOD.
7. IOD, na podstawie analizy zawartości Rejestru, a także w oparciu o inne pozyskane przez siebie informacje, sporządza i przedstawia Rektorowi raz na pół roku ogólną informację o stanie bezpieczeństwa informacyjnego Wyższej Szkoły Menedżerskiej w Warszawie, wraz ze stosownymi wnioskami. Odrębną część tej informacji stanowi opis stanu przestrzegania przepisów dotyczących ochrony danych osobowych. Wszystkie wskazane w niniejszym punkcie czynności stanowić winny również podstawę wszelkich poczynań w zakresie zarządzania ryzykiem informacyjnym w WSM.

VI. Uprawnienia Inspektora Ochrony Danych

1. W celu eliminowania negatywnych skutków naruszenia bezpieczeństwa informacyjnego w Wyższej Szkole Menedżerskiej w Warszawie, Inspektor Ochrony Danych ma prawo do podejmowania wymagających tego działań, a w szczególności:
   - żądania podania przez pracowników dodatkowych wyjaśnień w związku z zaistniałym zdarzeniem,

- korzystania z pomocy konsultantów,
- nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

2. Odmowa udzielenia wyjaśnień lub brak współpracy z IOD traktowana będzie jako poważne naruszenie podstawowych obowiązków pracowniczych.

VII. Postanowienia końcowe

1. Nieprzestrzeganie zasad i trybu postępowania określonych w niniejszej Instrukcji stanowi poważne naruszenie podstawowych obowiązków pracowniczych, które skutkować może możliwością nałożenia kary porządkowej przewidzianej przepisami kodeksu pracy. W przypadku osoby zatrudnionej na innej podstawie niż stosunek pracy możliwym będzie nałożenie kary przewidzianej treścią zawartej z nią umowy.
2. Osobą uprawnioną do określania wykładni przepisów niniejszej Instrukcji jest IOD. W przypadku utrzymującej się, mimo wyjaśnień IOD, różnicy w rozumieniu tych przepisów, ostatecznej wykładni dokonuje Rektor.
3. W przypadku wystąpienia sytuacji, która nie została przewidziana przepisami niniejszej Instrukcji, użytkownik ma oprawo zwrócić się do IOD z wnioskiem o określenie na piśmie sposobu wymaganego postępowania.

IX. Załączniki

Załącznik nr 1
Tabela form naruszeń bezpieczeństwa informacyjnego

Kod naruszenia	Formy naruszeń	Sposób postępowania
A	**Forma naruszenia bezpieczeństwa informacyjnego 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 IOD.
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 IOD.
A.1.3	Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką informację 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 IOD.
A.2	**W zakresie sprzętu i oprogramowania**	
A.2.1	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do informacji chronionych.	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport i powiadomić IOD.
A.2.2	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych, w szczególnie danych osobowych, przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska pracy przy komputerze. Pouczyć osobę, która dopuściła się takiej sytuacji. Sporządzić raport i powiadomić IOD.
A.2.3	Pozostawienie w miejscu niezabezpieczonym, a w szczególności miejscu widocznym, zapisanego hasła dostępu do systemu informatycznego.	Zabezpieczyć notatkę z hasłami w sposób uniemożliwiający jej odczytanie. Sporządzić raport i powiadomić IOD.
A.2.4	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami WSM.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały osoby nieuprawnione wykonane. Przerwać działanie programów. Sporządzić raport i powiadomić IOD.

A.2.5	Samodzielne instalowanie oprogramowania.	Pouczyć osobę wykonującą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne WSM w celu odinstalowania programów. Sporządzić raport i powiadomić IOD.
A.2.6	Modyfikowanie parametrów systemu i aplikacji	Wezwać osobę wykonującą wymienioną czynność, aby jej zaniechała. Sporządzić raport i powiadomić IOD.
A.2.7	Odczytywanie zewnętrznych nośników danych przed sprawdzeniem ich oprogramowaniem antywirusowym.	Pouczyć osobę wykonującą wymienioną czynność, aby stosowała się do wymogów bezpieczeństwa obowiązujących w tym zakresie.. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport i powiadomić IOD.
A.3	**W zakresie dokumentów i obrazów zawierających dane osobowe**	
A.3.1	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Sporządzić raport i powiadomić IOD.
A.3.2	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych.	Powiadomić przełożonych pracownika. Spowodować poprawę zastanej sytuacji. Sporządzić raport i powiadomić IOD.
A.3.3	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym odczytanie ich treści.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport i powiadomić IOD.
A.3.4	Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport i powiadomić IOD.
A.3.5	Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawniona osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały dane, w szczególności dane osobowe - sporządzić raport i powiadomić IOD.
A.3.6	Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych odrębnymi procedurami.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Sporządzić raport i powiadomić IOD.
A.3.7	Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Sporządzić raport i powiadomić IOD.
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 służący do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć (zamknąć) pomieszczenie. Powiadomić przełożonych. Sporządzić raport i powiadomić IOD.
A.4.2	Wpuszczanie do pomieszczeń służbowych osób nieznanych i	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich

	dopuszczanie ich do kontaktu ze sprzętem komputerowym.	tożsamość. Powiadomić przełożonych. Sporządzić raport i powiadomić IOD.
A.4.3	Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiekolwiek 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. Sporządzić raport i powiadomić IOD.
A.5	**W zakresie pomieszczeń, w których znajdują się serwery 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 dostępnych publicznie (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość z pomocą pracowników ochrony. Powiadomić służby informatyczne WSM. Sporządzić raport i powiadomić IOD.
A.5.2	Dopuszczanie do znalezienia się w pomieszczeniach serwerowni lub węzłów sieci informatycznej 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 WSM. Sporządzić raport i powiadomić IOD.
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 WSM. 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 WSM i IOD. 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 WSM oraz IOD. 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 WSM oraz IOD. 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 WSM oraz IOD. 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 obowiązującymi w tego rodzaju przypadkach procedurami. Powiadomić IOD i sporządzić raport.

C	**Formy naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem**	
C.1	Próba uzyskania hasła uprawniającego do dostępu do systemów, w których przetwarzane są dane osobowe, w ramach świadczenia pomocy technicznej.	Powiadomić IOD i sporządzić raport.
C.2	Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych, przy użyciu identyfikatora i hasła użytkownika.	Powiadomić IOD i sporządzić raport.

Załącznik nr 2
Wzór raportu o naruszeniu bezpieczeństwa informacyjnego.

Raport o naruszeniu bezpieczeństwa informacyjnego

Sporządzający raport:

Nazwisko i imię .....
Stanowisko i funkcja .....
Jednostka organizacyjna, pokój, nr telefonu .....

Kod formy naruszenia (wg tabeli) .....

1. Miejsce, dokładny czas i data stwierdzonego naruszenia (budynek, piętro, nr pokoju, godzina, itp.) :
   .....
   .....

2. Osoby powodujące naruszenie bezpieczeństwa informacyjnego:
   .....
   .....

3. Osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony bezpieczeństwa informacyjnego:
   .....
   .....

4. Informacje o danych, które zostały lub mogły zostać ujawnione:
   .....
   .....

5. Zabezpieczone materiały lub inne dowody związane z wydarzeniem:
   .....
   .....

6. Krótki opis wydarzenia związanego z naruszeniem bezpieczeństwa informacyjnego (przebieg zdarzenia, opis zachowania uczestników, podjęte działania):
   .....
   .....
   .....
   .....
   .....
   .....

....
data podpis

Załącznik nr 3

Wzór „Rejestru naruszeń bezpieczeństwa informacyjnego w WSM"

Lp	Czas trwania naruszenia			Osoba / źródło informacji o naruszeniu	Kategoria i liczba osób, których dotyczy naruszenie	Zakres danych i lub kategorie danych, których dotyczy naruszenie	Miejsce naruszenia	Sposób naruszenia	Opis charakteru naruszenia	Opis okoliczności naruszenia	Przyczyna naruszenia pośrednia i bezpośrednia	Osoba/podmiot odpowiedzialna za naruszenie	Podjęte działania korygujące i lub naprawcze	Osoba odpowiedzialna za wdrożenie działań naprawczych	Czy informowano TUDO ? Jeżeli tak to wskazać datę i podmiot zgłoszenia	Czy informowano osobę, której dotyczy naruszenie ?	Monitoring działań naprawczych
	Data i godzina rozpoczęcia naruszenia	Data i godzina stwierdzenia naruszenia	Data naruszenia (okres, którego dotyczy)														
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18