ZARZĄDZENIE NR 0050.112.2018
BURMISTRZA MIASTA ZAMBRÓW

z dnia 23 listopada 2018 r.

w sprawie wprowadzenia Polityki zarządzania ryzykiem utraty bezpieczeństwa danych

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz.U. z 2018r. poz. 994 ze zm.) i art. 24 ust 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zarządza się co następuje:

§ 1. Wprowadza się „Politykę zarządzania ryzykiem utraty bezpieczeństwa danych" stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Polityka reguluje postępowania pracowników Urzędu Miasta Zambrów zatrudnionych przy przetwarzaniu danych osobowych, definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie.

§ 3. Zobowiązuje się wszystkich pracowników do przestrzegania zasad i realizacji zadań określonych w polityce, o której mowa w § 1.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta

Kazimierz Dąbrowski

Załącznik do zarządzenia Nr 0050.112.2018

Burmistrza Miasta Zambrów z dnia 23 listopada 2018 r.

POLITYKA ZARZĄDZANIA RYZYKIEM UTRATY BEZPIECZEŃSTWA DANYCH

Niniejsza Polityka reguluje postępowanie pracowników Urzędu Miasta Zambrów zatrudnionych przy przetwarzaniu danych osobowych, definiuje katalog naruszeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie.

§ 1. Celem niniejszej instrukcji jest określenie zadań pracowników w zakresie:

1) ochrony danych osobowych przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą oraz ochroną zasobów technicznych;

2) prawidłowego reagowania pracowników zatrudnionych przy przetwarzaniu danych osobowych w przypadku stwierdzenia naruszenia ochrony danych osobowych lub zabezpieczeń systemu informatycznego;

3) ograniczenia ryzyka powstania zagrożeń oraz minimalizacja skutków wystąpienia zagrożeń.

Rozdział 1.
Opis zdarzeń naruszających ochronę danych

§ 2. 1. Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.

2. Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, Administratora, awarie sprzętowe, błędy oprogramowania), możliwe zniszczenie danych, zakłócenie ciągłości pracy systemu, możliwość naruszenia poufności danych.

3. Zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia, naruszenia poufności danych (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenia ciągłości pracy)zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

§ 3. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są informacje, to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np.: pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;

1) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy;

2) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;

3) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;

4) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;

5) naruszenie lub próba naruszenia integralności systemu lub bazy danych;

6) próba lub modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),

7) niedopuszczalna manipulacja danymi osobowymi w systemie;

8) ujawnienia osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń;

9) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.;

10) ujawnienia istnienia nieautoryzowanych kont dostępu do danych lub tzw. bocznej furtki itp.;

11) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane;

12) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych itp.);

13) za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne);

14) nielegalne bądź nieświadome ujawnienie danych osobowych;

15) pozyskiwanie danych osobowych z nielegalnych źródeł;

16) przetwarzanie danych osobowych niezgodne z uprawnionym celem i zakresem;

17) ujawnienie indywidualnych haseł dostępu do danych osobowych w systemie;

18) przesyłanie danych osobowych przez Internet bez zabezpieczenia;

19) dopuszczenie do przetwarzania danych osobowych pracowników bez odpowiednich upoważnień.

§ 4. O możliwości zaistnienia przypadku naruszenia zasad ochrony danych osobowych mogą świadczyć m.in.:

1) nadmierne, w stosunku do wykonywanych zadań (zakres upoważnienia), uprawnienia użytkownika do zasobów systemu,

2) niestabilna praca systemu, w którym przetwarza się dane osobowe,

3) korzystanie z zasobów systemu poza godzinami pracy (bez zgody przełożonego),

4) nowe „podejrzane" konta użytkowników,

5) wysoka aktywność kont, które długo pozostawały niewykorzystane,

6) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania (system jest tak skonfigurowany, iż po trzech próbach podania błędnego hasła wymaga interwencji Administratora),

7) anomalie w pracy systemu lub programu (świadczące np. o obecności wirusa),

8) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których przetwarza się dane osobowe (wyłamane lub zacinające się zamki, naruszone plomby, niedomykające się okna itp.),

9) nielegalne ujawnienie danych,

10) pozyskiwanie danych z nielegalnych źródeł.

Rozdział 2.
Postępowanie w przypadku naruszenia ochrony danych

§ 5. Naruszenie systemu ochrony danych osobowych może zostać stwierdzone na podstawie oceny:

1) stanu urządzeń technicznych;

2) zawartości zbiorów danych osobowych;

3) sposobu działania programu lub jakości komunikacji w sieci teleinformatycznej;

4) metod pracy (w tym obiegu dokumentów).

§ 6. Każdy pracownik Urzędu Miasta w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest bezzwłocznie powiadomić Inspektora ochrony danych lub bezpośredniego przełożonego.

§ 7. Inspektor ochrony danych lub inna upoważniona przez niego osoba podejmuje wszelkie działania mające na celu:

1) minimalizację negatywnych skutków zdarzenia,

2) wyjaśnienie okoliczności zdarzenia,

3) zabezpieczenie dowodów zdarzenia,

4) umożliwienie dalszego bezpiecznego przetwarzania danych.

§ 8. Inspektor ochrony danych oraz Administrator systemu informatycznego ocenia sytuację i podejmuje odpowiednie do potrzeb działania, a w szczególności:

1) dokonuje rozpoznania zdarzenia,

2) ocenia wagę problemu,

3) ocenia możliwość wystąpienia strat w zasobach informacyjnych i systemowych w przypadku dalszego działania systemu,

4) lokalizuje źródło problemu (przeprowadza analizę posiadanych danych).

§ 9. W celu realizacji zadań wynikających z niniejszej polityki Inspektor ochrony danych lub inna upoważniona przez niego osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:

1) żądania wyjaśnień od pracowników,

2) korzystania z pomocy konsultantów,

3) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

§ 10. Polecenia Inspektora ochrony danych lub innej upoważnionej przez niego osoby wydawane w celu realizacji zadań wynikających z niniejszej instrukcji są priorytetowe i winny być wykonywane przed innymi poleceniami, zapewniając ochronę danych osobowych.

§ 11. Odmowa udzielenia wyjaśnień lub współpracy z Inspektorem ochrony danych lub inną upoważnioną przez niego osobą traktowana będzie jako naruszenie obowiązków pracowniczych.

§ 12. Inspektor ochrony danych po zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości. Wzór raportu stanowi załącznik 1 do niniejszej Polityki.

§ 13. W przypadku stwierdzenia, że podejrzenie nie świadczy o naruszeniu zasad ochrony danych, Inspektor ochrony danych oraz Administrator systemu informatycznego po przeanalizowaniu sytuacji i wyeliminowaniu możliwości wystąpienia ich w przyszłości, podejmuje decyzję o dalszej pracy systemu.

§ 14. 1. W przypadku stwierdzenia naruszenia ochrony danych osobowych wciągu 72 godzin po jego stwierdzeniu Administrator zgłasza je organowi nadzorczemu – Prezesowi Urzędu Ochrony Danych Osobowych, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

2. Inspektor ochrony danych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze w rejestrze, którego wzór stanowi załącznik nr 2 do niniejszej Polityki.

3. Zgłoszenie naruszenia zabezpieczeń danych osobowych powinno zawierać:

1) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorię i przybliżoną liczbę osób, których dane dotyczą oraz kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

2) imię i nazwisko oraz dane kontaktowe Inspektora ochrony danych oraz oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji dotyczących naruszenia;

3) opis możliwych konsekwencji naruszenia ochrony danych osobowych;

4) opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

§ 15. Jeżeli w czasie usuwania skutków naruszenia bezpieczeństwa danych osobowych nastąpi czasowe obniżenie poziomu bezpieczeństwa systemu, po zakończeniu czynności naprawczych, system przetwarzający te dane powinien posiadać poziom bezpieczeństwa nie niższy niż poprzedni.

§ 16. Każda informacja o naruszeniu ochrony danych i jego okolicznościach, kierowana poza urząd, może być przekazana wyłącznie przez Administratora danych osobowych lub Inspektora ochrony danych.

§ 17. Polityka określa zasady postępowania wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych w przypadku naruszenia bezpieczeństwa tych danych. Formy naruszeń i sposoby postępowania w przypadku ich zaistnienia określa „Katalog naruszeń i incydentów zagrażających bezpieczeństwu danych osobowych", stanowiący załącznik nr 3 do niniejszej Polityki.

§ 18. Każda osoba dopuszczona do przetwarzania danych osobowych obowiązana jest zapoznać się z niniejszą Polityką.

§ 19. Nieprzestrzeganie zasad postępowania określonych w niniejszej Polityce stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.

Burmistrz Miasta

Kazimierz Dąbrowski

Załącznik Nr 1 do Polityki zarządzania ryzykiem utraty bezpieczeństwa danych

Wzór raportu z sytuacji naruszenia bezpieczeństwa danych osobowych

Sporządzający raport:

.....

(dane Inspektora ochrony danych)

Kod formy naruszenia ochrony danych .....
(wg. katalog naruszeń i incydentów zagrażających bezpieczeństwu danych osobowych)

1. Miejsce, dokładny czas i data naruszenia ochrony danych osobowych

.....

2. Osoby powodujące naruszenie, które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia ochrony danych osobowych:

.....

3. Osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych:

.....

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 ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania):

.....

.....

.....

7. Wnioski:

.....

.....

.....

.....

(data i podpis Inspektora ochrony danych)

.....

(data i podpis Administratora Danych Osobowych)

Załącznik Nr 2 do Polityki zarządzania ryzykiem utraty bezpieczeństwa danych

REJESTR NARUSZEŃ I INCYDENTÓW ZAGRAŻAJĄCYCH BEZPIECZEŃSTWU OCHRONY DANYCH

Numer raportu	Kod formy naruszenia	Osoba zgłaszająca	Osoba powodująca naruszenie	Podjęte działania	Wynik podjętych działań

Załącznik Nr 3 do Polityki zarządzania ryzykiem utraty bezpieczeństwa danych

KATALOG NARUSZEŃ I INCYDENTÓW ZAGRAŻAJĄCYCH BEZPIECZEŃSTWU DANYCH OSOBOWYCH

Zastosowane skróty:

ASI - Administrator Systemów Informatycznych

IOD - Inspektor Ochrony Danych

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 IOD.
A.1.2	Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Powiadomić IOD. Sporządzić raport z opisem, jaka informacja została ujawniona.
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. Powiadomić IOD. Sporządzić raport z opisem, jaka informacja została ujawniona.
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 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	Samodzielne instalowanie i wykorzystanie nielegalnego oprogramowania oraz narzędzi służących do obchodzenia zabezpieczeń w systemach informatycznych.	Pouczyć osobę popełniającą wymieniona czynność, aby jej zaniechała. Wezwać ASI w celu odinstalowania programów. Sporządzić raport.
A.2.6	Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymieniona czynność, aby jej zaniechała. Sporządzić raport.
A.2.7	Odczytywanie nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa ochrony danych. Wezwać ASI w celu wykonania kontroli antywirusowej. Sporządzić raport.
A.2.8	Wykorzystywanie ogólnodostępnych serwisów pocztowych (np. Wirtualna Polska, Onet.pl, gmail.com) w celach służbowych.	Nakazać osobie popełniającą wymienioną czynność korzystania jedynie z poczty służbowej. 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 do 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 IDO. Sporządzić raport.
A.3.7	Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić IDO. Sporządzić raport.
A.3.8	Udostępnienie danych osobowych osobom nieuprawionym.	Powiadomić IDO. 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 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 IDO. Sporządzić raport.
A.4.3	Dopuszczanie, aby osoby bez wiedzy ASI z firm informatycznych i telekomunikacyjnych podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji. Wyżej wymienione czynności powinny być konsultowane z ASI, a o ich zamiarze powinien zostać poinformowany pracownik sprawujący nadzór nad bezpieczeństwem budynku.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić ASI i IOD. Sporządzić raport.
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 IOD.
A.4.6	Nieprzestrzeganie polityki czystego biurka oraz czystego ekranu.	Nakazać osobie popełniającej wymienioną czynność postępowania według zasad panujących w Urzędzie. Powiadomić IOD.
	Pozostawienie dokumentów w koszu na śmieci.	Zabezpieczyć dokumenty. Przekazać informację IOD.
A.4.7	Pozostawienie wydruków na ogólnodostępnej drukarce.	Zabezpieczyć dokumenty. Przekazać informację IOD.

A.4.8.	Nieautoryzowane wykonanie kopii klucza do pomieszczeń biurowych.	Powiadomić IOD. Sporządzić raport.
A.4.9	Wyniesienie kluczy od pomieszczeń biurowych po zakończonej pracy.	Powiadomić 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 i ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.2	Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu	Powiadomić niezwłocznie AS. 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 ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.4	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych	Powiadomić niezwłocznie Administratora Systemu Informatycznego. 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 ASI. 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 przepisami – zawiadomić policję. Powiadomić niezwłocznie IOD. Sporządzić raport.
B.7	Przekazywanie haseł innym osobom.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD. Zmienić hasło do systemu.
B.8	Niewłaściwe niszczenie nośników z danymi pozwalającymi na ich odczyt.	Zabezpieczyć nośnik. Zawiadomić IOD.
B.9	Wykorzystanie służbowych środków przetwarzania informacji do celów prywatnych	Powiadomić niezwłocznie IOD.
B.10	Nadmierne uprawnienia w systemach w stosunku do wykonywanej pracy.	Powiadomić ASI lub IOD.
B.11	Nieuprawniona zmiana danych lub ich uszkodzenie.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.
B.12	Fizyczne zniszczenie lub uszkodzenie sprzętu oraz nośników przetwarzających informacje	Powiadomić niezwłocznie IOD i ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.
B.13	W wyniku rozwiązania umowy z pracownikiem nie podjęto działań związanych z odebraniem uprawnień	Powiadomić niezwłocznie ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.

B.14	Nieuprawniony dostęp do strefy administracyjnej	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić ASI. Sporządzić raport.
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 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 IOD. Sporządzić raport.