ZARZĄDZENIE Nr 96/2014
Burmistrza Bornego Sulinowa
z dnia 26 października 2014 r.

w sprawie wprowadzenia Procedury alarmowej i ustalenia zasad sporządzania Sprawozdania rocznego stanu systemu ochrony danych osobowych w ramach „Polityki bezpieczeństwa informacji w systemach informatycznych i kartotekach służących do przetwarzania danych osobowych w Urzędzie Miejskim w Bornem Sulinowie”

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2013 r., poz. 594 ze zm.) w związku z art. 36 ust. 12 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182) **zarządzam,** co następuje:

§ 1. 1. Wprowadzam do użytku „Procedurę alarmową” dotyczącą ochrony danych osobowych stanowiącą załącznik nr 1 do niniejszego zarządzenia.

2. Załącznik nr 1 nie podlega publikacji.

§ 2. 1. Ustalam zasady sporządzania „Sprawozdania rocznego stanu systemu ochrony danych osobowych” stanowiącego załącznik nr 2 do niniejszego zarządzenia

2. Załącznik nr 2 nie podlega publikacji.

§ 3. Zobowiązuje się pracowników Urzędu Miejskiego w Bornem Sulinowie do stosowania zasad określonych w w/w dokumentach

§ 4. Wykonanie zarządzenia powierzam Sekretarzowi Gminy.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

URZĄD MIEJSKI W BORNEM SULINOWIE

Załącznik nr 1
do Zarządzenia nr 96/2014
Burmistrza Bornego Sulinowa
z dnia 27.10.2014r

Procedura alarmowa

Ochrona danych osobowych
w Urzędzie Miejskim w Bornem Sulinowie

2014 rok

Spis treści:

1. Wstęp

Administrator Danych Osobowych w Urzędzie Miejskim w Bornem Sulinowie w celu pełnej kontroli oraz zapobiegania możliwym zagrożeniom związanym z ochroną danych osobowych na podstawie art. 36.1. ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285) wprowadza dokument o nazwie **„Procedura Alarmowa”**. Zapisy tego dokumentu obowiązują wszystkich pracowników Urzędu Miejskiego w Bornem Sulinowie, którzy przetwarzają dane osobowe w systemach informatycznych i w wersji papierowej.

Z niniejszym dokumentem powinni zapoznać się wszyscy pracownicy, a w szczególności:

1) kierownicy referatów i pracownicy z samodzielnych stanowisk pracy,
2) osoby upoważnione do przetwarzania danych osobowych w zbiorach i bazach danych,
3) obsługa informatyczna Urzędu Miejskiego.

Niniejsze procedury korespondują z dokumentem pn. Polityka Bezpieczeństwa Informacji w systemach informatycznych i kartotekach służących do przetwarzania danych osobowych w Urzędzie Miejskim w Bornem Sulinowie, która została wprowadzona Zarządzeniem nr 80/2012 Burmistrza Bornego Sulinowa z dnia 14 grudnia 2012 r.

Za rozpowszechnienie dokumentu i umożliwienie zapoznania się z nim przez wszystkich pracowników odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

Dokument powinien zostać umieszczony w formie elektronicznej, na wewnętrznych zasobach sieciowych Urzędu Miejskiego, do których dostęp posiadają wszyscy pracownicy Urzędu Miejskiego w Bornem Sulinowie lub w uzasadnionych przypadkach na żądanie powinien zostać im przedłożony w formie papierowej.

Podstawa prawna:

1) Ustawę z dn. 29.08.1997 r. o ochronie danych osobowych (ze zm.),

2) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3.06.1998 r. w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia Inspektora Ochrony Danych Osobowych (ze zm.),

3) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych,

2. Podstawowe definicje i pojęcia

ADO - Administrator Danych Osobowych **–** Burmistrz Bornego Sulinowa.

ABI - Administrator Bezpieczeństwa Informacji osoba wyznaczona przez Administratora Danych Osobowych do pełnienia funkcji Administratora Bezpieczeństwa Informacji.

ASI - osoba wyznaczona przez Administratora Danych Osobowych do pełnienia funkcji Administratora Systemu Informatycznego Urzędu Miejskiego w Bornem Sulinowie.

Użytkownik danych – każdy pracownik, który wykonując czynności służbowe, przetwarza dane osobowe, tzn. wykonuje na nich operacje takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie;

Osoba upoważniona – osoba posiadająca upoważnienie wydane przez ABI lub osobę uprawnioną przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym w zakresie wskazanym w upoważnieniu.

Osoba uprawniona – osoba posiadająca upoważnienie wydane przez ABI do wykonywania w jego imieniu określonych czynności.

Uchybienie - świadome lub nieświadome działania zmierzające do zagrożenia, wskutek których może dojść do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.

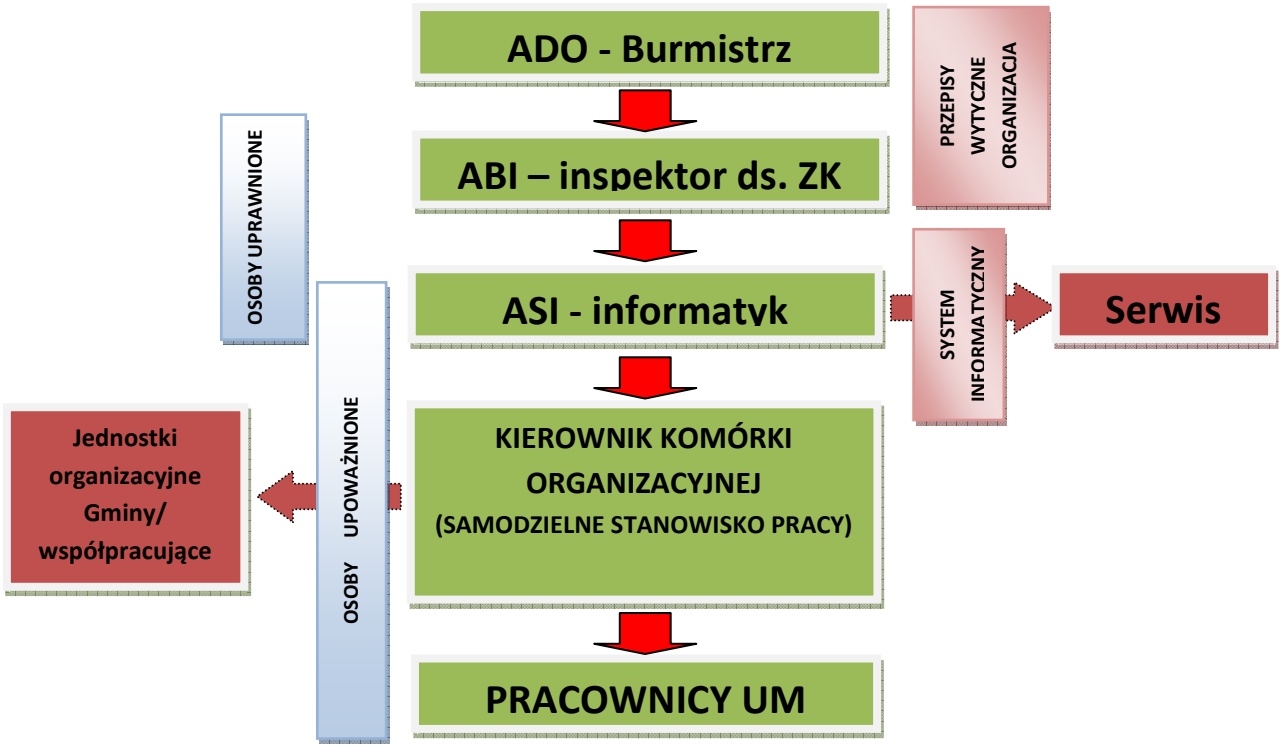
Zagrożenie - świadome lub nieświadome działania, wskutek których doszło do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.

Procedura alarmowa – sposób postępowania (rodzaj czynności) osób funkcyjnych i pracowników w sytuacji zagrożenia utraty danych osobowych przetwarzanych w Urzędzie Miejskim w Bornem Sulinowie.

3. Procedura alarmowa

Procedura alarmowa wskazuje na możliwe zagrożenia oraz definiuje **„Dziennik Uchybień i Zagrożeń”**, związany z niewłaściwym przetwarzaniem danych osobowych lub ich wyciekiem.
Celem Procedury Alarmowej jest skatalogowanie możliwych uchybień i zagrożeń oraz opisanie procedur działania w przypadku ich wystąpienia, jak i również ograniczenie ich powstania w przyszłości.
Częścią Procedury Alarmowej jest „**Dziennik Uchybień i Zagrożeń”** - (załącznik nr 1), **„Protokół Zagrożenia”** - (załącznik nr 2), oraz **„Protokół Uchybienia”** - (załącznik nr 3), Dokumenty prowadzone są przez ABI w przypadku stwierdzenia naruszenia ochrony danych osobowych w Urzędzie Miejskim w Bornem Sulinowie.

Reagowanie w sytuacji powstania uchybień i zagrożenia wiąże się ze strukturą uprawnień oraz zakresem odpowiedzialności za prawidłowe przetwarzanie danych osobowych w Urzędzie Miejskim w Bornem Sulinowie (rys. 1).



Rysunek 1 Struktura uprawnień oraz zakresu odpowiedzialności za prawidłowe przetwarzanie danych w Urzędzie Miejskim w Bornem Sulinowie

4. Charakterystyka możliwych „Uchybień i Zagrożeń”

4.1. Uchybienia i zagrożenia nieświadome wewnętrzne i zewnętrzne

Do uchybień i zagrożeń nieświadomych wewnętrznych i zewnętrznych należą działania pracowników Urzędu Miejskiego lub osób nie będących pracownikami Urzędu Miejskiego, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności.

W szczególności są to działania takie jak:
- niewłaściwe zabezpieczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
- niewłaściwe zabezpieczenie danych przetwarzanych na stanowisku pracy,
- niewłaściwe zabezpieczenie sprzętu komputerowego, włamanie do systemu,
- dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia,
- pomyłki informatyków, samowolna zmiana oprogramowania,
- wykorzystanie sprzętu do celów prywatnych z użyciem nie sprawdzonych nośników danych,
- brak reakcji na zagrożenia,
- kradzież danych,
- niewłaściwe przechowywanie, posługiwanie się oraz nieuprawnione udostępnianie haseł i kodów dostępu,
- pozostawienie bez opieki a w konsekwencji utrata lub kradzież sprzętu informatycznego,
- działanie wirusów i innego szkodliwego oprogramowania oraz inne działania, wskutek których dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.

5.2. Uchybienia i zagrożenia umyślne wewnętrzne i zewnętrzne

Do uchybień i zagrożeń umyślnych wewnętrznych i zewnętrznych należą celowe działania pracowników Urzędu Miejskiego, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności.

W szczególności są to działania takie jak:
- celowe zniszczenie sprzętu, danych osobowych lub nośników danych,
- kradzież lub utrata danych osobowych,
- dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia,
- nadmierne nadawanie uprawnień do dostępu do systemu i przetwarzanych danych osobowych,
- kradzież danych,
- zainfekowanie złośliwego oprogramowania,
- niewłaściwe niszczenie dokumentów,
- nie stosowanie obowiązujących procedur, brak szkolenia,
- kradzież sprzętu informatycznego,
- działanie wirusów i innego szkodliwego oprogramowania oraz inne działania, wskutek których dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.

5.3. Uchybienia i zagrożenia losowe

Do uchybień i zagrożeń losowych należą sytuacje losowe, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności.

W szczególności są to sytuacje takie jak:
- klęski żywiołowe,
- przerwy w dostawie prądu (zasilania),
- niesprawne źródła zasilania awaryjnego,
- awarie serwera i innych urządzeń wchodzących w skład systemu,
- pożar,
- zalanie wodą.

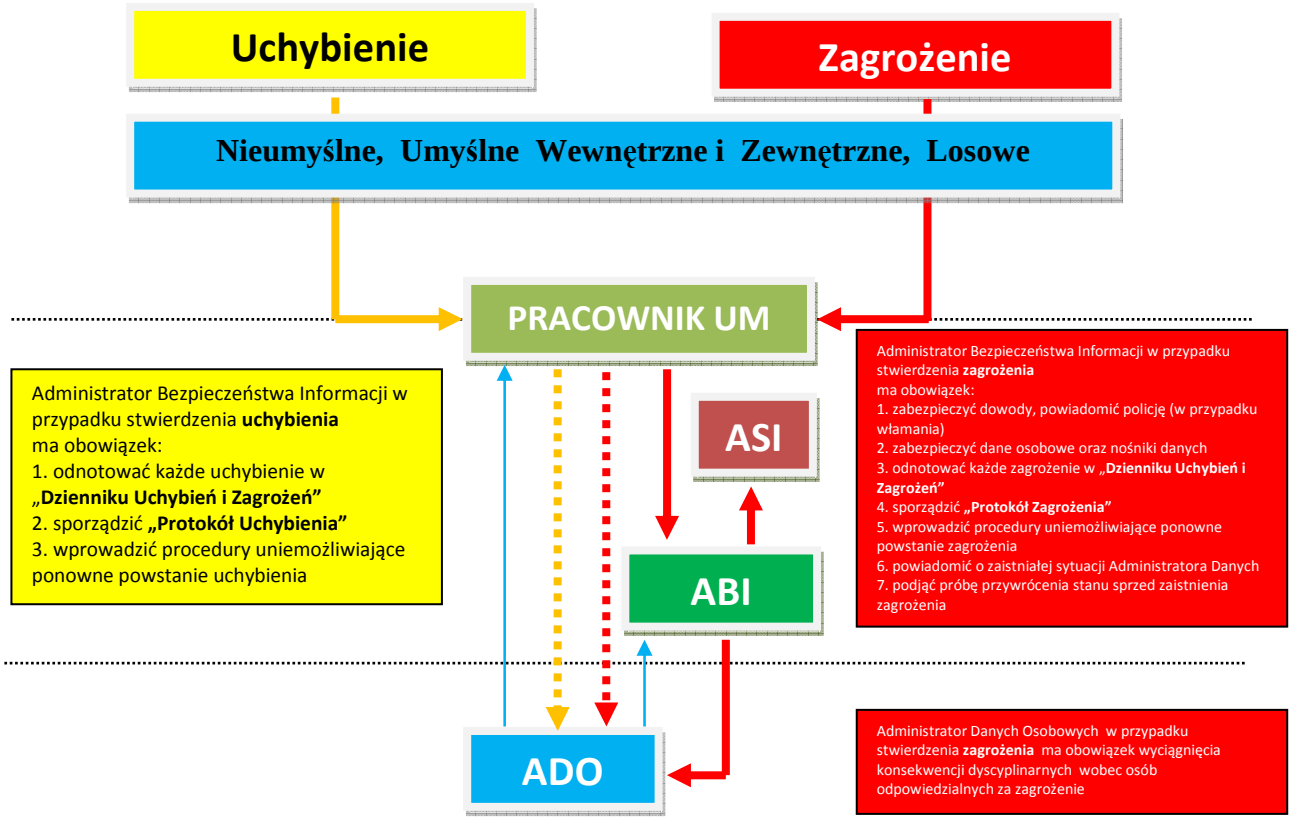
4.4. Procedura postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych.

Każdy pracownik Urzędu Miejskiego w Bornem Sulinowie posiadający upoważnienie do przetwarzania danych osobowych, w przypadku stwierdzenia uchybienia lub zagrożenia ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji lub Administratora Danych (rys 2).

Administrator Bezpieczeństwa Informacji w przypadku stwierdzenia **uchybienia** ma obowiązek:
- odnotować każde uchybienie w „**Dzienniku Uchybień i Zagrożeń”,**
- sporządzić **„Protokół Uchybienia”,**
- wprowadzić procedury uniemożliwiające ponowne powstanie uchybienia.

Administrator Bezpieczeństwa Informacji w przypadku stwierdzenia **zagrożenia** ma obowiązek:
zabezpieczyć dowody, powiadomić policję (w przypadku włamania)
- zabezpieczyć dane osobowe oraz nośniki danych,
- odnotować każde zagrożenie w „**Dzienniku Uchybień i Zagrożeń”**
- sporządzić **„Protokół Zagrożenia”**
- wprowadzić procedury uniemożliwiające ponowne powstanie zagrożenia
- powiadomić o zaistniałej sytuacji Administratora Danych
- podjąć próbę przywrócenia stanu sprzed zaistnienia zagrożenia.

Administrator Danych Osobowych w przypadku stwierdzenia zagrożenia może wyciągnąć konsekwencje dyscyplinarne wobec osób odpowiedzialnych za zagrożenie.



Rysunek 2 Postępowanie w przypadku naruszenia ochrony danych osobowych.

Szczegółowy zakres incydentów związanych z bezpieczeństwem informacji w wyniku których może dojść do utraty danych osobowych określa Polityka Bezpieczeństwa Informacji.

4. Rejestr uchybień i zagrożeń oraz szczegółowa instrukcja postępowania dla osób posiadających upoważnienie do przetwarzania danych osobowych w Urzędzie Miejskim

Kod uchybienia lub zagrożenia	Uchybienia i zagrożenia nieświadome, świadome wewnętrzne i zewnętrzne oraz zdarzenia losowe	Postępowanie w przypadku uchybienia lub zagrożenia
01	Pomieszczenie, środki do przetwarzania danych osobowych pozostają bez nadzoru.	Należy zabezpieczyć dane osobowe oraz powiadomić ABI. ABI sporządza protokół uchybienia.
02	Pominięto system kontroli dostępu do stref administracyjnych Urzędu Miejskiego i pomieszczeń teletechnicznych.	Należy zabezpieczyć pomieszczenia i powiadomić ABI. ABI sporządza protokół zagrożenia i powiadamia ADO.
03	Pozostawienie niezabezpieczonych pomieszczeń, szaf w których przechowywane są dane osobowe oraz dokumentów na biurkach po zakończeniu pracy.	Należy zabezpieczyć dane osobowe, pomieszczenia i powiadomić ABI. ABI sporządza protokół uchybienia.
04	Dokumenty i nośniki elektroniczne zawierające dane osobowe nie zostały zniszczone w sposób uniemożliwiający ich odczyt, pozostawiono je koszu naśmieci lub nie odebrano wydruków z drukarek ogólnodostępnych.	Należy zabezpieczyć dane osobowe, nośniki, dokumenty i powiadomić ABI. ABI sporządza protokół uchybienia.
05	Zgubiono klucze, lub wykonano kopie kluczy do pomieszczeń biurowych w których przechowuje się dane osobowe, nie zachowując obowiązującej procedury.	Należy zabezpieczyć dane osobowe, pomieszczenia i powiadomić ABI. ABI sporządza protokół zagrożenia i powiadamia ADO.
06	Zidentyfikowano lub wykorzystywano środek przetwarzający informacje nieznanego pochodzenia (sprzęt, nośniki) oraz wykonywanie zdalnej pracy przy pomocy komputera inny niż służbowy.	Należy zabezpieczyć dane osobowe, sprzęt i powiadomić ABI. Należy zabezpieczyć sprzęt. ABI sporządza protokół zagrożenia lub uchybienia, powiadamia ADO adekwatnie do sytuacji.
07	Niestosowanie się do wymagań dotyczących złożoności haseł, przechowywanie ich w sposób niewłaściwy lub nieuprawnione ich udostępnianie.	Należy zabezpieczyć dane osobowe, sprzęt i powiadomić ABI. ASI zmienia hasło dostępu. ABI sporządza protokół zagrożenia i powiadamia ADO.
08	Pojawienie się nieautoryzowanej informacji na stronie internetowej.	Należy zabezpieczyć dane osobowe i powiadomić ABI. ABI sporządza protokół zagrożenia i powiadamia ADO, ASI identyfikuje źródło informacji.

09	Podjęto pracę w stanie zagrożenia bezpieczeństwa informacji (m.in. próba logowania za pomocą nieprawidłowego hasła) w wyniku czego zostało zablokowane konto użytkownika.	Należy zabezpieczyć dane osobowe, sprzęt i powiadomić ABI. ABI sporządza protokół zagrożenia i powiadamia ADO.
10	Stwierdzono wykorzystywanie służbowej poczty do celów prywatnych oraz ogólnopolskich serwisów pocztowych w celach służbowych.	Należy zabezpieczyć dane osobowe i powiadomić ABI. ABI sporządza protokół uchybienia.
11	Komputer nie jest zabezpieczony hasłem.	Należy zabezpieczyć dane osobowe oraz powiadomić ABI. ABI sporządza protokół uchybienia.
12	Stwierdzono wykorzystywanie nielegalnego lub złośliwego oprogramowania (wirusa, atak hackera) oraz narzędzi służących do obchodzenia zabezpieczeń w systemie informatycznym, próby instalacji nie zatwierdzonego oprogramowania lub zmiany konfiguracji sprzętowej oraz programowej systemów oraz stacji roboczych przez nieupoważnione osoby.	Należy zabezpieczyć dane osobowe, sprzęt i powiadomić ABI. ABI sporządza protokół zagrożenia i powiadamia ADO.
13	Nie zgłaszane są przypadki nieprawidłowego działania systemów bezpieczeństwa.	Należy powiadomić ABI. ABI sporządza protokół uchybienia.
14	Dostęp do danych osobowych mają osoby nieposiadające upoważnienia, pracownik nie podpisał oświadczeń.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI. ABI sporządza protokół uchybienia.
15	Nie anulowano uprawnień pracownikowi, z którym wygasła, rozwiązano umowę o pracę, nie rozliczył się z powierzonych materiałów i środków przetwarzania informacji.	Należy zabezpieczyć dane osobowe i powiadomić ABI. ABI sporządza protokół uchybienia.
16	Brak zabezpieczeń w umowach ze stronami trzecimi z którymi wiąże się przetwarzanie danych osobowych lub umożliwienie stronie wykonywanie czynności na terenie Urzędzie Miejskim w wyniku, której może dojść do utraty danych (serwisanci).	Należy zabezpieczyć dane osobowe i powiadomić ABI. ABI sporządza protokół zagrożenia i powiadamia ADO.
17	Utrata danych osobowych w wyniku kradzieży, zagubienia, nieuprawnionego przekazania.	Należy zabezpieczyć dane osobowe i powiadomić ABI. ABI sporządza protokół zagrożenia.

18	Nadawanie nadmiernych uprawnień dostępu do systemów przetwarzających dane osobowe.	Należy powiadomić ABI. ABI sporządza protokół uchybienia.
19	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym.	Należy powiadomić ABI, który powinien sprawdzić system uwierzytelniania oraz sprawdzić czy nie doszło do kradzieży lub zniszczenia danych. ABI sporządza protokół uchybienia.
20	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych.	Należy nie dopuścić do kradzieży danych i powiadomić ABI. ABI powinien zabezpieczyć nośnik danych i powiadomić ADO. ABI sporządza protokół zagrożenia i powiadamia ADO.
21	Próba kradzieży danych osobowych w formie papierowej.	Należy nie dopuścić do kradzieży danych i powiadomić ABI. ABI powinien zabezpieczyć dane i powiadomić ADO. ABI sporządza protokół zagrożenia i powiadamia ADO.
22	Nieuprawniony dostęp do danych osobowych w formie papierowej.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI. ABI sporządza protokół uchybienia.
23	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu.	Należy powiadomić ABI. ABI powinien zabezpieczyć pomieszczenie. ABI sporządza protokół uchybienia.
24	Próba włamania do pomieszczenia/budynku, kradzieży sprzętu przetwarzającego dane osobowe.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. ABI sporządza protokół zagrożenia i powiadamia ADO.
25	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania.	Należy zrobić audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych, firewall. ABI powinien ocenić, czy nie doszło do utraty danych osobowych i w zależności od tego sporządzić protokół uchybienia lub zagrożenia.
26	Brak aktywnego oprogramowania antywirusowego.	Należy powiadomić ABI. ABI powinien zaktualizować lub nabyć oprogramowanie antywirusowe. ABI sporządza protokół uchybienia.

27	Nieuprawniona zmiana, zniszczenie lub modyfikacja danych osobowych w formie papierowej.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia ADO. ABI sporządza protokół zagrożenia.
28	Nieuprawniona zmiana, zniszczenie , uszkodzenie, (w tym sprzętu oraz nośników przetwarzających dane osobowe) lub modyfikacja danych osobowych w systemie informatycznym.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia ADO. ABI sporządza protokół zagrożenia.
29	Awaria systemu informatycznego, uszkodzenie komputerów, nośników danych.	Należy powiadomić ABI. ABI powinien ocenić w wyniku czego doszło do zniszczenia i przywrócić dane z kopii zapasowej. ABI powiadamia ADO i sporządza protokół zagrożenia.
30	Próba nieuprawnionej interwencji przy sprzęcie komputerowym.	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić ABI. ABI sporządza protokół uchybienia
31	Utrudniona dostępność systemu informatycznego spowodowana awarią zasilania urządzeń przetwarzających informacje, obciążeniem procesora, przekroczenie dostępnych zasobów systemowych, itp.	Należy zabezpieczyć dane osobowe, pomieszczenia i powiadomić ABI. ABI sporządza protokół uchybienia.
32	Błędy w obsłudze i konserwacji sprzętu komputerowego oraz przechowywaniu, eksploatacji i konserwacji oprogramowania.	Należy zabezpieczyć sprzęt i oprogramowania i powiadomić ABI. ABI sporządza protokół uchybienia.
33	Nie wykonywane są kopie bezpieczeństwa ora nie weryfikuje się możliwości odtworzenia danych z kopii zapasowych.	Należy zabezpieczyć dane osobowe, pomieszczenia i powiadomić ABI. ABI sporządza protokół zagrożenia i powiadamia ADO.
34	Zdarzenia losowe (pożar, zalanie, klęska żywiołowa).	Powiadomić ABI i ASI. ABI oszacowuje powstałe starty i sporządza protokół zagrożenia lub uchybienia i powiadamia ADO.

Załącznik nr 1

do Procedury Alarmowej

DZIENNIK UCHYBIEŃ I ZAGROŻEŃ

Kod	**Data i godzina zdarzenia**	**Rodzaj zdarzenia *(uchybienie/ zagrożenie)***	**Opis zdarzenia**	**Skutki zdarzenia**	**Działania naprawcze**	**Podpis ABI**

Załącznik nr 2
do Procedury Alarmowej

Urząd Miejski w Bornem Sulinowie Borne Sulinowo, dnia …… 20 … r.

ul. Al. Niepodległości 6

PROTOKÓŁ ZAGROŻENIA

Data i godzina wystąpienia zagrożenia - .....

Kod zagrożenia - .....

Opis zagrożenia

.....
.....
.....
.....
.....

Przyczyny powstania zagrożenia

.....
.....
.....
.....
.....

Zaistniałe skutki zagrożenia

.....
.....
.....
.....
.....

Podjęte działania naprawczo-zapobiegawcze

.....
.....
.....

Administrator Bezpieczeństwa Informacji **Administrator Danych Osobowych**

…..... .....

Podpis Podpis

Załącznik nr 3
do Procedury Alarmowej

Urząd Miejski w Bornem Sulinowie
ul. Al. Niepodległości 6

Borne Sulinowo, dnia …… 20 … r.

PROTOKÓŁ UCHYBIENIA

Data i godzina wystąpienia uchybienia - .....

Kod uchybienia - .....

Opis uchybienia

.....
.....
.....
.....
.....

Przyczyny powstania uchybienia

.....
.....
.....
.....
.....

Zaistniałe skutki uchybienia

.....
.....
.....
.....
.....

Podjęte działania naprawczo-zapobiegawcze

.....
.....
.....
.....
.....

Administrator Bezpieczeństwa Informacji

….....
Podpis

Administrator Danych Osobowych

.....
Podpis