

**INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA  
BEZPIECZEŃSTWA DANYCH OSOBOWYCH  
GIMNAZJUM nr 1 w ŻARACH**

**§ 1**

Celem instrukcji jest określenie sposobu postępowania gdy:

1. Stwierdzono naruszenie zabezpieczeń danych osobowych.
2. W przypadku danych przetwarzanych w formie tradycyjnej stan pomieszczeń, szaf, okien, drzwi, dokumentów lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.
3. W przypadku danych przetwarzanych w formie elektronicznej stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu, jakość komunikacji lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.

**§ 2**

Instrukcja określa zasady postępowania wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych w przypadku naruszenia bezpieczeństwa tych danych, zgodne z „Tabelą form naruszeń bezpieczeństwa danych osobowych”, stanowiącą załącznik A do niniejszej instrukcji.

**§ 3**

Naruszeniem zabezpieczenia danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub usunięcia, a w szczególności:

- a) nieautoryzowany dostęp do danych,
- b) nieautoryzowane modyfikacje lub zniszczenie danych,

- c) udostępnienie danych nieautoryzowanym podmiotom,
- d) nielegalne ujawnienie danych,
- e) pozyskiwanie danych z nielegalnych źródeł.

#### § 4

1. W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych w jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie zgłosić ten fakt bezpośrednio przełożonemu, Administratorowi Bezpieczeństwa Informacji lub Lokalnemu Administratorowi Bezpieczeństwa informacji, a następnie postępować stosownie do podjętej przez niego decyzji.
2. Zgłoszenie naruszenia zabezpieczeń danych osobowych powinno zawierać:
  - a) opisanie symptomów naruszenia zabezpieczeń danych osobowych,
  - b) określenie sytuacji i czasu w jakim stwierdzono naruszenie zabezpieczeń danych osobowych,
  - c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia,
  - d) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

#### § 5

Administrator Bezpieczeństwa Informacji lub inna upoważniona przez niego osoba podejmuje wszelkie działania mające na celu:

- a) minimalizację negatywnych skutków zdarzenia,
- b) wyjaśnienie okoliczności zdarzenia,
- c) zabezpieczenie dowodów zdarzenia,
- d) umożliwienie dalszego bezpiecznego przetwarzania danych.

## **§ 6**

W celu realizacji zadań wynikających z niniejszej instrukcji Administrator Bezpieczeństwa Informacji lub inna upoważniona przez niego osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:

- a) żądania wyjaśnień od pracowników,
- b) korzystania z pomocy konsultantów,
- c) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

## **§ 7**

Polecenia Administratora Bezpieczeństwa Informacji 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.

## **§ 8**

Odmowa udzielenia wyjaśnień lub współpracy z Administratorem Bezpieczeństwa Informacji lub inną upoważnioną przez niego osobą traktowana będzie jako naruszenie obowiązków pracowniczych.

## **§ 9**

Administrator Bezpieczeństwa Informacji 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 B do niniejszej instrukcji.

## **§ 10**

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

## **§ 11**

Jeżeli skutkiem działania określonego w §10 jest ujawnienie informacji osobie nieupoważnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej

wynikającej z przepisów Kodeksu Karnego.

## § 12

Jeżeli skutkiem działania określonego w §10 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Prawa Cywilnego.

Żary, dn. 10.09.2013

.....  
(podpis dyrektora)

## Tabela form naruszeń bezpieczeństwa danych osobowych

| Kod naruszenia | Formy naruszeń   | Sposób postępowania   |
|----------------|--|---|
| <b>A</b>       | <b>Forma naruszenia ochrony danych osobowych przez pracownika zatrudnionego przy przetwarzaniu danych</b>  |   |
| <b>A.1</b>     | <b>W zakresie wiedzy:</b>  |   |
| 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.                   |
| <b>A.2</b>     | <b>W zakresie sprzętu i oprogramowania</b>   |   |
| 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          | <p>Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiegokolwiek inne osoby niż osoba, której identyfikator został przydzielony</p> <p>Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Sporządzić raport.</p> |   |
| 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  | Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji. |

|              |  |   |
|--------------|--|---|
|              | pracownikami   | Sporządzić raport.  |
| A.2.5        | Samodzielne instalowanie jakiegokolwiek oprogramowania.  | Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Sporządzić raport.   |
| A.2.6        | Modyfikowanie parametrów systemu i aplikacji.  | Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Sporządzić raport.   |
| A.2.7        | Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym.   | Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport. |
| <b>A.3.1</b> | <b><i>W zakresie dokumentów i obrazów zawierających dane osobowe</i></b>   |   |
| 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        | Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.  |   |
|              | Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.   |   |
| 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.3.6        | Utrata kontroli nad kopią danych osobowych   | Podjąć próbę odzyskania kopii. Powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.  |
| <b>A.4</b>   | <b><i>W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych</i></b>  |   |
| 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 komputerowym   | Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich 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.                                       |
| <b>A.5</b> | <b><i>W zakresie pomieszczeń w których znajdują się komputery centralne i urządzenia sieci.</i></b>  |  |
| 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.5.1      | 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>B</b>   | <b>Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych</b>  |  |
| 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.   |
| <b>C</b>   | <b>Formy naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem</b>  |  |
| 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.  |

Załącznik B  
do „Instrukcji postępowania w sytuacji naruszenia  
bezpieczeństwa danych osobowych”

**Wzór raportu końcowego sporządzanego przez administratora bezpieczeństwa informacji po  
zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych**

**Raport**

**o sytuacji naruszenia bezpieczeństwa danych osobowych**

**Sporządzający raport:**

Imię i nazwisko: .....

stanowisko (funkcja) .....

Dział, pokój, nr telefonu .....

**Kod formy naruszenia ochrony danych** ..... (wg tabeli)

1) Miejsce, dokładny czas i data naruszenia ochrony danych osobowych (piętro, nr pokoju, godzina, itp.): .....

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:

.....  
.....

.....  
(miejsce, data i godzina sporządzenia raportu)

.....  
(podpis sporządzającego raport)