REGULAMIN OCHRONY DANYCH

OSOBOWYCH

w Zespole Szkół Ponadgimnazjalnych im. Ignacego Wyssogoty Zakrzewskiego w Żelechowie

I. PODSTAWOWE POJĘCIA

1. Polityka bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. nr 101 poz. 926, ze zm.) oraz rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., nr 100, poz. 1024. Opracowany dokument jest zgodny z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.
2. Regulamin niniejszy określa tryb i zasady ochrony danych osobowych przetwarzanych w Zespole Szkół Ponadgimnazjalnych im. Ignacego Wyssogoty Zakrzewskiego w Żelechowie, zwanym dalej jednostką.
3. Ilekroć w regulaminie jest mowa o:
   a) **Jednostce** – rozumie się przez to Zespół Szkół Ponadgimnazjalnych im. Ignacego Wyssogoty Zakrzewskiego w Żelechowie;
   b) **Zbiorze danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
   c) **Danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
   d) **Przetwarzaniu danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
   e) **Systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
   f) **Systemie tradycyjnym** – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
   g) **Zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
   h) **Usuwaniu danych** – rozumie się prze to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
   i) **Administratorze danych osobowych** – w świetle art. 3 i 7 pkt. 4 ustawy o ochronie danych osobowych rozumie się przez to Dyrektora Jednostki, który decyduje o celach i środkach przetwarzania danych osobowych;

j) **Administratorze bezpieczeństwa informacji** – rozumie się przez to osobę wyznaczoną przez Dyrektora Jednostki, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych prze ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

k) **Administratorze systemu informatycznego** – rozumie się przez to osobę zatrudnioną prze Dyrektora Jednostki, upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;

l) **Użytkowniku systemu informatycznego** – rozumie się przez to upoważnionego przez Dyrektora Jednostki, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył stosowne szkolenie w zakresie ochrony tych danych;

m) **Zgodzie osoby, której te dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie – zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o inne treści.

II. CELE

Celem opracowania polityki bezpieczeństwa jest ochrona przed niepowołanym dostępem do:

a) Systemu informatycznego oraz informacji udostępnianych z jego wykorzystaniem;

b) Informacji zgromadzonych, przetwarzanych w formie tradycyjnej.

Niniejsze opracowanie określa politykę bezpieczeństwa w zakresie przetwarzania danych osobowych przez pracowników Jednostki, a w szczególności Kierowników/Dyrektorów komórek organizacyjnych oraz administratorów systemów informatycznych.

Dane osobowe w Jednostce są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Jednostki na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

Powyższy dokument wprowadza regulacje w zakresie zasad organizacji procesu przetwarzania i odnosi się swoją treścią do informacji:

a) w formie papierowe – przetwarzanej w ramach SYSTEMU TRADYCYJNEGO;

b) w formie elektronicznej – przetwarzanej w ramach SYSTEMU INFORMATYCZNEGO;

Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują Kierownicy komórek organizacyjnych.

Z zapisami w polityce bezpieczeństwa danych osobowych obowiązkowo są zapoznawani wszyscy użytkownicy systemów informatycznych i tradycyjnych.

Do informacji przechowywanych w systemach informatycznych jak i dokumentów tradycyjnych mają dostęp jedynie upoważnieni pracownicy Jednostki oraz osoby mające imienne zarejestrowane upoważnienie. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy. Dopuszczalny sposób i zakres przetwarzania danych osobowych regulują zapisy ustaw kompetencyjnych, szczegółowych właściwych dla komórek organizacyjnych Jednostki.

Dane osobowe są chronione zgodnie z polskim prawem oraz procedurami obowiązującymi w instytucjach samorządowych dotyczącymi bezpieczeństwa i poufności przetwarzanych danych. Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione odpowiednimi środkami technicznymi. Opracowane procedury określają obowiązki użytkownika zbiorów tradycyjnych oraz zasady korzystania z systemów informatycznych. Każdy użytkownik systemu informatycznego zobowiązany jest zapamiętać swoją nazwę użytkownika oraz hasło i nie udostępniać go innym osobom. Użytkownik systemu informatycznego powinien pamiętać o wylogowaniu się po zakończeniu korzystania z usług systemów informatycznych.

III. INFORMACJE OGÓLNE

Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada administrator danych osobowych. Kierownicy komórek organizacyjnych obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą utratą, uszkodzeniem lub zniszczeniem.

Administrator danych może wyznaczyć administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony. Prowadzi on dokumentację opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.

IV. ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

Administrator Bezpieczeństwa Informacji wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi i tradycyjnymi.

Administrator Bezpieczeństwa Informacji jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, iż wyłącznie autoryzowany personel ma dostęp do systemów informatycznych i tradycyjnych. Ponadto, w uzgodnieniu z kierownikami komórek organizacyjnych, określa warunki oraz sposób przydzielania użytkownikom kont i haseł. Administrator Bezpieczeństwa Informacji posiada bieżącą listę osób upoważnionych do przetwarzania danych osobowych.

Szczegółowy zakres odpowiedzialności i obowiązków Administratora Bezpieczeństwa Informacji jest następujący:

a) Nadzoruje bezpieczeństwo systemów informatycznych i tradycyjnych;
b) Nadzoruje przestrzeganie przez wszystkich użytkowników stosowanie obowiązujących procedur;
c) Weryfikuje listę autoryzowanych użytkowników systemów informatycznych;
d) Doradza użytkownikom w zakresie bezpieczeństwa;
e) Zapewnia, aby cały personel posiadający dostęp do systemu posiadał stosowne zezwolenia oraz był przeszkolony w zakresie obowiązujących regulacji bezpieczeństwa;
f) Przygotowuje i prowadzi „Ewidencję osób biorących udział w przetwarzaniu danych osobowych";
g) Prowadzi kontrole w zakresie bezpieczeństwa;
h) Przygotowuje wnioski pokontrolne dla Administratora.

V. UŻYTKOWNIK SYSTEMU

Użytkownik systemu wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem stacji roboczej. Jest odpowiedzialny przed Administratorem Bezpieczeństwa Informacji za nadzór, implementację i utrzymanie niezbędnych warunków bezpieczeństwa w szczególności do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

VI. POZIOM BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W SYTSEMIE INFORMATYCZNYM

Do grupy danych osobowych przetwarzanych w Jednostce jako pojedyncze informacje, w zestawach lub zbiorach w postaci papierowej ustala się zabezpieczenia na poziomie podstawowym.

Do grupy danych osobowych przetwarzanych w systemach informatycznych, ustala się zabezpieczenia na poziomie podstawowym.

VII. ZBIORY DANYCH OSOBOWYCH W JEDNOSTCE

Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Jednostki w postaci dokumentów papierowych.

Do przetwarzania zbiorów danych osobowych w systemie informatycznym Jednostki, stosowane są pakiety biurowe lub specjalizowane aplikacje (programy):

1. W szkole tworzy się następujące zbiory danych osobowych:

Zbiór nr 1 – Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych
Zbiór nr 2 – Zbiór upoważnień.
Zbiór nr 3 – Protokoły Rady Pedagogicznej.
Zbiór nr 4 – Arkusz organizacji roku szkolnego. (wersja papierowa i elektroniczna)
Zbiór nr 5 – Księga druków ścisłego zarachowania.
Zbiór nr 6 – Akta osobowe pracowników.
Zbiór nr 7 – Akta osobowe pracowników – rejestr elektroniczny "Kadry"
Zbiór nr 8 – Ewidencja zwolnień lekarskich pracowników AO.
Zbiór nr 9 – Ewidencja zwolnień lekarskich prac. pedagogicznych
Zbiór nr 10 – Księga zastępstw nauczycieli.
Zbiór nr 11 – Ewidencja urlopów pracowników niepedagogicznych.
Zbiór nr 12 – Ewidencja legitymacji pracowniczych.
Zbiór nr 13 – Ewidencja legitymacji ubezpieczeniowych.
Zbiór nr 14 – Ewidencja wydawanej pracownikom odzieży ochronnej.
Zbiór nr 15 – Rejestr delegacji służbowych.
Zbiór nr 16 – Dokumenty księgowe (wersja papierowa)
Zbiór nr 17 - Rejestr elektroniczny "Księgowość"
Zbiór nr 18 – Ewidencja osób korzystających ze świadczeń Funduszu Socjalnego
Zbiór nr 19 – Rejestr elektroniczny przyznanych świadczeń z Funduszu Socjalnego
Zbiór nr 20 – Listy płac pracowników – wydruki z komputera
Zbiór nr 21 - Rejestr elektroniczny "Płace"
Zbiór nr 22 - Ewidencja Kasy Zapomogowo-Pożyczkowej
Zbiór nr 23 - Rejestr elektroniczny Kasy Zapomogowo-Pożyczkowej
Zbiór nr 24 – Księga ewidencji uczniów.
Zbiór nr 25 – Ewidencja uczniów– Rejestr elektroniczny "Sekretariat szkoły"
Zbiór nr 26 - Lista mieszkańców internatu
Zbiór nr 27 – Dokumenty uczniów
Zbiór nr 28 – Ewidencja wydanych legitymacji szkolnych.
Zbiór nr 29 – Arkusze ocen wszystkich uczniów wraz z opiniami poradni PPP
Zbiór nr 30 – Dokumentacja zdrowotna uczniów.
Zbiór nr 31 – Zwolnienia lekarskie uczniów z wychowania fizycznego.
Zbiór nr 32 – Rejestr wypadków uczniów.
Zbiór nr 33 – Rejestr pedagoga szkolnego.
Zbiór nr 34 – Dzienniki lekcyjne i pozalekcyjne.
Zbiór nr 35 – Elekroniczne Dzienniki lekcyjne i pozalekcyjne .
Zbiór nr 36 – Protokoły egzaminów klasyfikacyjnych i poprawkowych.
Zbiór nr 37 – Ewidencja wydanych świadectw ukończenia szkoły.
Zbiór nr 38 - Lista uczniów zgłoszonych do egzaminu maturalnego oraz egzaminu zawodowego
Zbiór nr 39 - Dokumentacja egzaminu maturalnego oraz egzaminu zawodowego
Zbiór nr 40 - Rejestr elektroniczny uczniów zgłoszonych do egz. maturalnego oraz egz. zawodowego
Zbiór nr 41 – Ewidencja osób korzystających z księgozbioru bibliotecznego.
Zbiór nr 42 - Rejestr elektroniczny "Inwentarz"
Zbiór nr 43 – Archiwum (akta osobowe pracowników, listy płac, księgi arkuszy ocen, dzienniki lekcyjne)

2. Komunikacja:

- obieg dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi Jednostki, winien odbywać się w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).

3. Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie upoważnieni pracownicy oraz administrator systemu zapewniający jego prawidłową eksploatację. Wszyscy pracownicy, będący użytkownikami systemu zobowiązani są do zachowania danych w tajemnicy.

a) ochronie podlegają dane osobowe gromadzone i przechowywane w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych oraz w urządzeniach i systemie informatycznym Jednostki;

b) pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych, to znaczy posiadać odpowiednie zamki do drzwi, zabezpieczenia w oknach (w szczególności na parterze) oraz być wyposażone w środki ochrony ppoż.

c) dokumenty i nośniki informacji, zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieuprawnionych do przetwarzania danych. Jeżeli nie są aktualnie używane powinny być przechowywane w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia.

3. Zasady zabezpieczania danych:

- zbiory kartotekowe winny znajdować się w pomieszczeniach zabezpieczonych przed dostępem osób nieupoważnionych;

4. 1). Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest **dyrektor Grzegorz Szymczak** (administrator danych osobowych) lub pracownik posiadający wymagane prawem upoważnienie.

2) W przypadku udostępniania danych osobowych w celach innych niż włączenie do zbioru, administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

5. Należy mieć świadomość, że każdy, kto ma dostęp do pomieszczenia, w którym zainstalowano sprzęt systemu informatycznego może spowodować jego uszkodzenie lub może mieć dostęp do informacji wyświetlanych na monitorze lub wydruków.

Zagrożenia w stosunku do systemu mogą pochodzić również od każdej innej osoby, np. personelu pomocniczego, technicznego, konsultant itp. posiadającej wystarczające umiejętności i wiedzę, aby uzyskać dostęp do sieci.

6. Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa.

Hasło podlega szczególnej ochronie. Użytkownik ma obowiązek tworzenia haseł o długości minimum 8 znaków, nie trywialnych, tzn. nie może używać imion, danych identyfikacyjnych użytkownika oraz jego najbliższych, numerów rejestracyjnych, marek lub typów swoich samochodów itp., oraz nie może tworzyć haseł przez kombinację tych nazw lub ich zmianę uporządkowania np. od tyłu. Jest

wprowadzony wymóg zabraniający dokonywania zapisów haseł przez użytkowników. W przypadku, gdy użytkownik zapomni swoje hasło, może on uzyskać nowe hasło od Administratora Systemu zgodnie z obowiązującą procedurą.

7. Informacja przetwarzania i przechowywania w systemie musi być zabezpieczona w szczególny sposób.

   Środki bezpieczeństwa fizycznego są konieczne dla zapobiegania niepowołanemu dostępowi do informacji, nieautoryzowanym operacjom w systemie, kontroli dostępu do zasobów oraz w celu zabezpieczenia sprzętu teleinformatycznego.

8. Obszarem do przetwarzania danych osobowych z użyciem sprzętu komputerowego są:
   - sekretariat – część pomieszczeń za biurkami pracowników,
   - gabinet dyrektora,
   - gabinet wicedyrektorów,
   - gabinet kierownika Internatu,
   - gabinet kierownika szkolenia praktycznego,
   - gabinet pedagoga szkolnego,
   - biblioteka szkolna,
   - pokój nauczycielski (w zakresie dziennika elektronicznego),
   - sale lekcyjne (w zakresie dziennika elektronicznego),
   - pomieszczenia głównego księgowego,
   - pomieszczenie pracownika ds. kadr i płac.
   - Pokój administracyjny nr 19

   Przebywanie osób nieuprawnionych wewnątrz obszaru, o którym mowa w pkt. 8 jest dopuszczalna tylko w obecności osób zatrudnionych przy przetwarzaniu tych danych i za zgodą ABI.

9. Ochrona serwera, stacji roboczych i nośników.

   Pomieszczenia, w których znajdują się stanowiska komputerowe są:

   a) Zamknięte, jeśli nikt w nich nie przebywa;
   b) Wyposażone w sejfy lub inne pojemniki umożliwiające przechowywanie dokumentów.

10. Zasady kontroli sprzętu.

    Instalacja urządzeń systemu i sieci teleinformatycznej odbywa się za wiedzą i pod kontrolą Dyrektora komórki organizacyjnej, który jest również odpowiedzialny za warunki wprowadzania do użycia, przechowywania, eksploatacji oraz wycofania z użycia każdego urządzenia.

11. Sprzęt i oprogramowanie, indywidualnie lub łącznie mają ścisły związek z bezpieczeństwem systemu i sieci teleinformatycznej. Dlatego, powinny być ściśle przestrzegane procedury bezpieczeństwa odnoszące się do tych elementów.

12. Sieć teleinformatyczna jest organizacyjnym i technicznym połączeniem systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi. Niedopuszczalne jest samowolne przemieszczanie lub zmiana konfiguracji stacji roboczej bez wiedzy kierownika/dyrektora komórki organizacyjnej.

13. Nie zezwala się na korzystanie z jakiegokolwiek nowego oprogramowania bez zgody Administratora Systemu. Dodatkowe oprogramowanie może być zainstalowane wyłącznie po uzyskaniu zezwolenia Administratora Systemu. Kopie oprogramowania operacyjnego, aplikacyjnego i użytkowego przechowuje się w szafie metalowej znajdującej się w Sali nr 19

    Używanie oprogramowania prywatnego w sieci jest kategorycznie zabronione. Na stacjach roboczych powinno być zainstalowane jedynie niezbędne oprogramowanie.

14. Każde urządzenie użytkowe w systemie informatycznym, powinno podlegać rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez uprawnione osoby.

15. Za konserwację oprogramowania systemowego oraz aplikacyjnego serwera systemu informatycznego odpowiedzialny jest Administrator Systemu. Konserwacja ww. oprogramowania obejmuje także jego aktualizację.

    Za konserwacje oprogramowania stanowisk roboczych odpowiedzialny jest kierownik/dyrektor komórki organizacyjnej. Wszelkie aktualizacje oprogramowania powinny być uzgadniane z Administratorem Systemu.

16. Administrator Systemu przed rozpoczęciem naprawy urządzenia przez zewnętrzne firmy sprawdza, czy spełnione są następujące wymagania:

    a) w przypadku awarii serwera i konieczności oddania sprzętu do serwisu, nośniki magnetyczne zawierające dane osobowe powinny być wymontowane i do czasu naprawy serwera przechowywane w szafie metalowej znajdującej się w strefie o ograniczonym dostępie;

    b) w przypadku uszkodzenia nośnika magnetycznego zawierającego dane osobowe należy komisyjnie dokonać jego zniszczenia.

17. Serwer systemu oraz poszczególne stacje robocze (opcjonalnie) powinny być zabezpieczone urządzeniami podtrzymującymi zasilanie (UPS), co umożliwi funkcjonowanie systemu w przypadku awarii zasilania.

18. W celu zabezpieczenia ciągłości pracy, informacja przechowywana i przetwarzana w systemie podlega codziennej, przyrostowej archiwizacji (opcjonalnie) oraz pełnej archiwizacji przeprowadzanej nie rzadziej niż raz na dwa tygodni. Kopie archiwalne danych są wykonywane na nośnikach magnetooptycznych, i przechowywane są przez Administratora Systemu. Użycie kopii zapasowych następuje na polecenie Administratora Systemu w przypadku odtwarzania systemu po awarii.

Sugerowane działania:

- odłączenie urządzeń,
- zmiana haseł,
- odtworzenie z ostatnich kopii awaryjnych (w przypadku uszkodzenia baz danych),
- przywrócenie prawidłowego stanu działania systemu.

VIII. Załączniki do Regulaminu

- **Załącznik nr 1** - Lista uprawnionych do dostępu do zbiorów danych osobowych, wykaz miejsc przechowywania oraz sposobów zabezpieczenia zbiorów danych,
- **Załącznik nr 2** - Upoważnienie dla administratora bezpieczeństwa informacji,
- **Załącznik nr 3** - Upoważnienie dla administratora systemu informatycznego,
- **Załącznik nr 4** – Upoważnienie/Odwołanie upoważnienia dla pracownika do dostępu do danych osobowych,
- **Załącznik nr 5** – Oświadczenie pracownika o zapoznaniu z przepisami o ochronie danych osobowych,
- **Załącznik nr 6** - Rejestr osób uprawnionych do przetwarzania danych osobowych
- **Załącznik nr 7 -** Lista oświadczeń o zapoznaniu się z przepisami Ustawy o ochronie danych osobowych .

……..

podpis Administratora Bezpieczeństwa Informacji

	R A P O R T	Numer:
	z naruszenia zabezpieczenia danych osobowych w systemie przetwarzania danych osobowych	……..…
Oryginał/Kopia nr:	Komórka organizacyjna dokonująca zgłoszenia	

Data i godzina otrzymania informacji o naruszeniu (włamaniu do systemu),	(dzień, miesiąc, rok) godzina ……

Opis jego przebiegu:		
Ustalenia dotyczące charakteru i rodzaju naruszenia oraz metody działania osób naruszających zabezpieczenie systemu		
Przyczyny oraz wnioski ze zdarzenia:		