POLITYKA BEZPIECZEŃSTWA

PRZY PRZETWARZANIU DANYCH OSOBOWYCH

W ZESPOLE SZKÓŁ EKOLOGICZNYCH IM. UNII EUROPEJSKIEJ

W ZIELONEJ GÓRZE

Dział I.

Polityka Bezpieczeństwa

1. Polityka bezpieczeństwa rozumiana jest jako wykaz praw i zasad regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Zespołu Szkół Ekologicznych im. Unii Europejskiej w Zielonej Górze. Obejmuje całokształt zagadnień związanych z problemem zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie jak i w systemach informatycznych. Wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

Rozdział 1

Przepisy ogólne

§ 1

1. Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartym w ustawie z dnia 29 sierpnia 1997 r. *o ochronie danych oso*bowych (Dz. U. z 2002r. Nr 101, poz. 926 ze zm.) oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. *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 2004r. Nr 100, poz. 1024).

2. Polityka Bezpieczeństwa w zakresie ochrony danych osobowych w Zespole Szkół Ekologicznych im. Unii Europejskiej w Zielonej Górze odnosi się do danych osobowych przetwarzanych w zbiorach danych:

1) tradycyjnych, prowadzonych w formie papierowej, tzw. ręcznej;

2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.

3. Administrator danych mając świadomość, iż przetwarza dane **wrażliwe** uczniów deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.

4. W celu zabezpieczenia danych osobowych przed nieuprawnionym udostępnieniem Administrator danych wprowadza określone niniejszym dokumentem zasady przetwarzania danych. Zasady te określa w szczególności Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Dokumenty te są uzupełniane załącznikami do dokumentacji, na które składają się m.in.: wykazy zbiorów, miejsc ich przetwarzania oraz osób upoważnionych do przetwarzania danych.

5. W celu zapewnienia prawidłowego monitorowania przetwarzania danych wprowadza się liczne ewidencje, które szczegółowo charakteryzują obszary objęte monitoringiem, umożliwiając pełną kontrolę nad tym, jakie dane i przez kogo są przetwarzane oraz komu udostępniane.

6. Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest, aby każdy pracownik upoważniony do przetwarzania danych pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich.

7. W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.

§ 2

Ilekroć w niniejszym dokumencie jest mowa o:

1) Szkoła – należy przez to rozumieć Zespół Szkół Ekologicznych im. Unii Europejskiej w Zielonej Górze z siedzibą przy ul. Francuskiej 25a;

2) Administratorze Danych tzw. ADO – należy przez to rozumieć dyrektora Zespołu Szkół Ekologicznych im. Unii Europejskiej w Zielonej Górze;

3) Administratorze Bezpieczeństwa Informatycznego tzw. ABI– należy przez to rozumieć osobę wyznaczoną do nadzorowania przestrzegania zasad ochrony określonych w niniejszym

dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;

4) Administratorze Systemu Informatycznego tzw. ASI – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego w szkole oraz stosowanie technicznych i organizacyjnych środków ochrony;

5) Użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym szkoły, użytkownikiem może być pracownik szkoły, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej;

6) sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych w szkole wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci Telekomunikacyjnych;

7) sieci rozległej – należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 16 lipca 2004r. Prawo telekomunikacyjne (Dz. U. z 2004r., Nr 171, poz. 1800 ze zm.).

§ 3

1. Na podstawie § 4 pkt 2 Rozporządzenia 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 tworzy się ewidencję zbiorów osobowych wraz ze wskazaniem programów komputerowych służących do ich przetwarzania zgodnie z załącznikiem nr 1 do niniejszej dokumentacji.

Z uwagi na połączenie komputerów z siecią Internet, dla zbiorów przetwarzanych elektronicznie stosuje się, zgodnie z § 6 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. środki bezpieczeństwa na poziomie **WYSOKIM**.

2. Na podstawie § 4 pkt 1 Rozporządzenia 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 tworzy się wykaz pomieszczeń tworzących obszar fizyczny przetwarzania danych.

Wyznaczają go pomieszczenia zlokalizowane w Szkole. Szczegółowy wykaz pomieszczeń, stanowi załącznik nr 2 do niniejszej dokumentacji.

3. Zgodnie z art. 39 ust. 1 ustawy o ochronie danych osobowych wprowadza się ewidencję osób upoważnionych do przetwarzania danych, która stanowi załącznik nr 3 do niniejszej dokumentacji.

Ewidencja zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania uprawnień oraz zakres upoważnienia.

Ewidencja stanowi podstawę wydania Upoważnienia do przetwarzania danych osobowych na mocy art. 37 ustawy o ochronie danych osobowych.

Rozdział 2

Administracja i organizacja bezpieczeństwa

Informacje ogólne

§ 1

1. Za bezpieczeństwo danych osobowych przetwarzanych w systemie tradycyjnym i informatycznym odpowiada dyrektor Zespołu Szkół Ekologicznych im. Unii Europejskiej w Zielonej Górze – Administrator Danych.
2. Administrator Danych obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Rozdział 3

Środki organizacyjne ochrony danych osobowych

§ 1

1. W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:

a) Przetwarzanie danych osobowych w Szkole może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.

b) Zgodnie z art. 36 ust. 3 ustawy o ochronie danych osobowych, Administrator danych powołuje Administratora Bezpieczeństwa Informacji tzw. ABI (zał. nr10).

c) Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie. Wzór upoważnienia stanowi załącznik nr 4 do niniejszej dokumentacji.

d) ABI prowadzi ewidencję osób upoważnionych**,** o której mowa w pkt 5.5 oraz na jej podstawie przygotowuje Upoważnienia do przetwarzania danych i przedkłada je do podpisu ADO.

e) Unieważnienie upoważnienia następuje na piśmie, wg wzoru stanowiącego załącznik nr 5 do niniejszej dokumentacji.

f) Zabrania się przetwarzania danych poza obszarem określonym w załączniku nr 2 do niniejszej instrukcji.

g) Każdy pracownik Szkoły co najmniej raz na 2 lata musi odbyć szkolenie z zakresu ochrony danych osobowych. Za organizację szkoleń odpowiedzialny jest ADO, który prowadzi w tym celu odpowiednią dokumentację. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych.

h) Ponadto każdy upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Wzór potwierdzenia stanowi załącznik nr 6 do niniejszej dokumentacji. Podpisany dokument jest dołączany do akt osobowych.

i) Obszar przetwarzania danych osobowych określony w załączniku nr 2 do niniejszej dokumentacji, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

j) Przebywanie osób, nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą ADO lub w obecności osoby upoważnionej do przetwarzania danych osobowych. Wzory zgody na przebywanie w pomieszczeniach dla osób nie posiadających upoważnienia, a także odwołania tej zgody, stanowią odpowiednio załącznik nr 7 oraz załącznik nr 8 do przedmiotowej dokumentacji.

k) Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.

l) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

m) Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.

n) Przetwarzanie danych podawanych dobrowolnie może odbywać się tylko na podstawie pisemnej zgody podającego te dane wg wzoru określonego w załączniku nr 10.

§ 2

Dla zapewnienia kontroli przestrzegania zasad określonych w niniejszej dokumentacji wyznacza się następujące zadania Administratorowi Bezpieczeństwa Informacji tzw. ABI:

1. Nadzór nad przetwarzaniem danych zgodnie z ustawą o ochronie danych osobowych i innymi przepisami prawa.
2. Kontrola przestrzegania zasad ochrony – systematycznie, nie rzadziej niż dwa razy do roku kontrolowanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności kontrola pod kątem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, w szczególności:
    a) Kontrola dokumentacji opisującej sposób przetwarzania oraz ochrony.
    b) Kontrola fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są informacje.
    c) Kontrola poprawności zabezpieczeń danych przetwarzanych metodami tradycyjnymi.
    d) Kontrola awaryjnego zasilania komputerów.
    e) Nadzór nad naprawą, konserwacją oraz likwidacją urządzeń komputerowych.
    f) Kontrola systemu kontroli obecności wirusów komputerowych.
    g) Kontrola wykonywania kopii awaryjnych.
    h) Kontrola przeglądu, konserwacji oraz uaktualnienia systemów informatycznych.
    i) Kontrola mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych.
    j) Kontrola nadanych upoważnień.

3. Przedstawianie ADO wyników kontroli.

4. Systematyczna analiza dokumentacji pod kątem obszarów, zbiorów oraz zasad ochrony.
5. Podjęcie natychmiastowych działań zabezpieczających w przypadku otrzymania informacji o naruszeniu bezpieczeństwa informacji. Zagrożenie bezpieczeństwa opisano formy naruszenia zbiorów i tryb dalszego postępowania opisano w załącznik nr 12 do niniejszego dokumentu.
6. Prowadzenie monitoringu przetwarzania danych.
7. Każdorazowe sporządzenie raportu zgodnie ze wzorem będącym załącznikiem nr 9 do niniejszej dokumentacji oraz przedstawienie efektów działań Administratorowi danych.

Rozdział 4.

Środki techniczne ochrony danych osobowych

§ 1

Zbiory danych przetwarzane w Szkole zabezpiecza się poprzez:

I. Środki ochrony fizycznej.

1. Zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi) .
2. Serwerownia , w której przetwarzane są zbiory danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.
3. Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej niemetalowej szafie.
4. Kopie zapasowe zbiorów danych osobowych przechowywane są w zamkniętej niemetalowej szafie.
5. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

II. Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej.

1. Zbiory danych osobowych przetwarzane są przy użyciu komputera przenośnego oraz stacjonarnego
2. Komputery służące do przetwarzania danych osobowych jest połączony z lokalną siecią komputerową.
3. Zastosowano urządzenia typu UPS, i wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
4. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
5. Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
6. Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.
7. Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
8. Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
9. Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
10. Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
11. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
12. Użyto system Firewall do ochrony dostępu do sieci komputerowej.

III. Środki ochrony w ramach systemowych narzędzi programowych i baz danych.

1. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbiorów danych osobowych.
2. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanych zbiorów danych osobowych.
3. Dostęp do zbiorów danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

4. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
5. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbiorów danych osobowych.
6. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
7. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Dodatkowe środki ochrony technicznej systemu informatycznego, jak również wszystkie niezbędne informacje dotyczące jego pracy oraz zasad użytkowania, określa Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych opisana w Dziale II niniejszego dokumentu.

Dział II.

Instrukcja zarządzania systemem informatycznym

Rozdział 1.

§ 1

I. CHARAKTERYSTYKA SYSTEMU

1. Sieć informatyczna ma strukturę gwiazdy, do której podłączony jest serwer oraz komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe.
2. Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony.

§ 2

II. OGÓLNE ZASADY PRACY W SYSTEMIE INFORMATYCZNYM

1. ADO wyznacza Administratora Systemu Informatycznego zwanym dalej ASI wg .wzoru załącznik nr 13.

2. ASI odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych.
3. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez ASI do eksploatacji licencjonowane oprogramowanie.
4. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:
    a. mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika, z pominięciem narzędzi do edycji tekstu,
    b. mechanizmy ochrony poufności, dostępności i integralności informacji, z uwzględnieniem potrzeby ochrony kryptograficznej,
    c. mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,
    d. mechanizmy monitorowania w celu identyfikacji i zapobiegania zagrożeniom, w szczególności pozwalające na wykrycie prób nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie,
5. Użytkownikom zabrania się:
    a. korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy Szkoły bez pisemnej zgody ADO,
    b. udostępniania stanowisk roboczych osobom nieuprawnionym,
    c. wykorzystywania sieci komputerowej Szkoły w celach innych niż wyznaczone przez ADO,
    d. samowolnego instalowania i używania programów komputerowych,
    e. korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,
    f. umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej Szkoły oraz sieci Internetowej osobom nieuprawnionym,
    g. używania komputera bez zainstalowanego oprogramowania antywirusowego.

§ 3

III. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI.

1. Użytkowników systemu informatycznego tworzy oraz usuwa ASI na podstawie zgody ADO.
2. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.
3. Wprowadza się rejestr osób upoważnionych do przetwarzania danych osobowych, który stanowi załącznik nr 3 do Polityki Bezpieczeństwa w Zespole Szkół Ekologicznych im. Unii Europejskiej w Zielonej Górze.
4. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku:
    a. zawieszenia w pełnieniu obowiązków służbowych.
5. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.
6. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.

§ 4

IV. STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM.

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.
2. Konto użytkownika systemu informatycznego składa się z imienia i nazwiska użytkownika zarejestrowanego..
3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika ASI, nadaje inny identyfikator odstępując od ogólnej zasady.

4. W identyfikatorze pomija się polskie znaki diakrytyczne.
5. Hasło składa się z co najmniej ośmiu znaków, zawiera co najmniej jedną literę wielką, jedną cyfrę.
6. Zmianę hasła należy dokonywać nie rzadziej niż co 30 dni.
7. Hasło nie może być zapisywane i przechowywane.
8. Użytkownik nie może udostępniać identyfikatora oraz haseł osobom nieupoważnionym.

§ 5

V. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY.

1. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.
2. Użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami nie mającymi uprawnień.
3. Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu. Użytkownik jest zobowiązany w takiej sytuacji do włączenia wygaszacza ekranu odblokowywanego hasłem.
4. Zabrania się opuszczania stanowiska pracy bez wcześniejszego wylogowania z systemu z zastrzeżeniem pkt 3.
5. Zakończenie pracy polega na wylogowaniu się z systemu i wyłączeniu komputera.
6. ASI monitoruje logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.

§ 6

VI. PROCEDURY TWORZENIA KOPII AWARYJNYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA.

1. Dane osobowe zabezpiecza się poprzez wykonywanie kopii awaryjnych.

2. Ochronie poprzez wykonanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych. Kopie programów i narzędzi wykonywane są zaraz po instalacji oraz po każdej aktualizacji na zewnętrznych, elektronicznych nośnikach informacji.
3. Zabezpieczeniu poprzez wykonywanie kopii awaryjnych podlegają także dane konfiguracyjne systemu informatycznego przetwarzającego dane osobowe, w tym uprawnienia użytkowników systemu.
4. Za proces tworzenia kopii awaryjnych na serwerze odpowiada ASI.
5. W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych, użytkownicy systemu informatycznego zobowiązani są do wykonywania samodzielnie kopii bezpieczeństwa tych zbiorów.
6. Kopie awaryjne mogą być sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze.
7. Kopie awaryjne wykonuje się codziennie.
8. Kopie awaryjne przechowuje ASI, a w przypadku przetwarzania danych na stacjach roboczych poszczególni użytkownicy.
9. Wszelkie wydruki zawierające dane osobowe powinny być przechowywane w miejscu uniemożliwiającym ich odczyt przez osoby nieupoważnione, zaś po upływie czasu ich przydatności – niszczone w niszczarkach dokumentów.

§ 7

VII. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI.

1. Dane osobowe gromadzone są wyłącznie serwerze. Zabrania się gromadzenia danych osobowych na innych nośnikach danych.
2. W uzasadnionych przypadkach, za zgodą ABI, dane osobowe można przetwarzać na dyskach twardych komputerów stacjonarnych lub zarejestrowanych nośnikach informacji dostarczonych przez ASI.
3. Przenośne nośniki danych powinny być zabezpieczone ochroną kryptograficzną.
4. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

a. **likwidacji** — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

b. **przekazania podmiotowi nieuprawnionemu do przetwarzania danych** — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,

c. **naprawy** — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ASI.

5. Nośniki kopii awaryjnych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym przez ABI.

§ 8

VIII. SPOSÓB ZABEZPIECZENIA SYSTEMU PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO.

1. ASI zapewnia ochronę antywirusową oraz zarządza systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody. System antywirusowy jest skonfigurowany w następujący sposób:

   a. skanowanie dysków zawierających potencjalnie niebezpieczne dane następuje automatycznie po włączeniu komputera,

   b. skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej jest realizowane na bieżąco.

   c. Automatycznej aktualizacji wzorców wirusów.

2. W przypadkach wystąpienia infekcji użytkownik powinien niezwłocznie powiadomić o tym fakcie ASI.

3. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ASI podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

   a. usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,

   b. odtworzenie plików z kopii awaryjnych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,

c. samodzielną ingerencję w zawartość pliku - w zależności od posiadanych narzędzi i oprogramowania.

4. Użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
5. ASI monitoruje stan systemu, ruch użytkowników w sieci oraz próby ingerencji z zewnątrz w system.

§ 9

IX. INFORMACJE O ODBIORCACH, KTÓRYM DANE OSOBOWE ZOSTAŁY UDOSTĘPNIONE, DACIE I ZAKRESIE TEGO UDOSTĘPNIENIA.

1. Informacje o udostępnieniu danych osobowych przetwarza się i przechowuje w oparciu o Jednolity Rzeczowy Wykaz Akt i Instrukcję kancelaryjną.
2. Za udostępnianie danych zgodnie z przepisami prawa odpowiedzialny jest ADO.
3. Nadzór nad właściwym udostępnianiem danych prowadzi ABI.

§ 10

X. PRZESYŁANIE DANYCH POZA OBSZAR PRZETWARZANIA

1. Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez zastosowanie ochrony kryptograficznej.
2. W wypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych należy zastosować szczególne środki bezpieczeństwa, które obejmują:
    a. zatwierdzenie przez ASI zakresu danych osobowych przeznaczonych do wysłania,
    b. zastosowanie mechanizmów szyfrowania danych osobowych,
3. Umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.

§ 11

XI. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH.

1. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez ADO.
2. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez ASI.
3. W przypadku uszkodzenia zestawu komputerowego, nośniki danych, na których są przechowywane dane osobowe powinny zostać zabezpieczone przez ASI.
4. W przypadku konieczności przeprowadzenia prac serwisowych poza Szkołą, dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać w sposób trwały usunięte.
5. Jeżeli nie ma możliwości usunięcia danych z nośnika na czas naprawy komputera, należy zapewnić stały nadzór nad tym nośnikiem przez osobę upoważnioną do przetwarzania danych osobowych na nim zgromadzonych.
6. ASI wykonuje okresowy przegląd nośników danych osobowych eliminując te, które nie zapewniają odpowiedniego poziomu bezpieczeństwa oraz niezawodności.

Dział III.

Rozdział 1.

Znajomość polityki bezpieczeństwa przy przetwarzaniu danych osobowych

§ 1

Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy Zespołu Szkół Ekologicznych im. Unii Europejskiej w Zielonej Górze upoważnieni do przetwarzania danych osobowych.

ZAŁĄCZNIKI:

Załącznik nr 1.Ewidencja zbiorów osobowych przetwarzanych w Szkole.

Załącznik nr 2. Ewidencja miejsc przetwarzania zbiorów osobowych w Szkole.

Załącznik nr 3. Ewidencja osób upoważnionych do przetwarzania danych osobowych w Szkole.

Załącznik nr 4. Wzór upoważnienia do przetwarzania danych osobowych.

Załącznik nr 5. Wzór unieważnienia upoważnienia do przetwarzania danych osobowych.

Załącznik nr 6. Wzór potwierdzenia znajomości zasad bezpieczeństwa.

Załącznik nr 7. Wzór zgody na przebywanie w obszarze przetwarzania danych osobowych.

Załącznik nr 8. Wzór odwołania zgody na przebywanie w obszarze przetwarzania danych osobowych.

Załącznik nr 9. Wzór raportu z naruszenia bezpieczeństwa zasad ochrony danych osobowych.

Załącznik nr 10. Wzór powołania Administratora Bezpieczeństwa Informacji.

Załącznik nr 11. Wzór zgody na przetwarzanie danych.

Załącznik nr 12 - Wzór powołania Administratora Systemu Informatycznego.

ZAWTIERDZAM:

Data: ……

Administrator Danych Osobowych

……

(podpis i pieczęć)

Załącznik nr 1.

EWIDENCJA ZBIORÓW OSOBOWYCH i opis struktur i programu

Lp.	Nazwa zbioru - opis	Podstawa prawna przetwarzania	Struktura zbioru	Program	Zgłoszenie GIODO
1.	Księga Ewidencji Dzieci w Szkole Podstawowej - Coroczna adnotacja o spełnianiu przez dziecko obowiązku szkolnego w tej albo innej szkole	§ 3a.2. pkt 1) rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. 2002,nr 23, poz.225 z późn.zm.)	Imię (imiona) i nazwisko, datę i miejsce urodzenia oraz adres zamieszkania dziecka, a także imiona i nazwiska rodziców (prawnych opiekunów) oraz adresy ich zamieszkania, pesel	VULCAN	TAK
2.	Księga Ewidencji Dzieci w Gimnazjum - Coroczna adnotacja o spełnianiu przez dziecko obowiązku szkolnego w tej albo innej szkole	§ 3b.2. pkt 1) rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. 2002, nr 23, poz.225 z późn.zm)	Imię (imiona) i nazwisko, datę i miejsce urodzenia oraz adres zamieszkania dziecka, a także imiona i nazwiska rodziców (prawnych opiekunów) oraz adresy ich zamieszkania, pesel	VULCAN	TAK
3.	Karta zapisu dziecka do szkoły - Informacje dot. ucznia przyjmowanego do szkoły	§ 4.1. rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r. z późn. zm.), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, pesel, wizerunek dziecka, telefon	System „NABÓR”	NIE (art. 43.1. pkt 4)
4.	Księga Ewidencji Uczniów - Zbiór danych o uczniach	§ 4.1. rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r. z późn. zm.), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, pesel zawód, przyjęcie do szkoły: data, klasa semestr, obwód szkolny, profil kierunek zawód specjalność Wypisanie ze szkoły: data, klasa, powody, Data: wydania dok, ukończenia szkoły numer wydanego świadectwa (dyplomu)	VULCAN	NIE (art. 43.1. pkt 4)
5.	Dziennik lekcyjny - Dokumentacja przebiegu nauczania w danym roku szkolnym	§ 7.2. rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r. z późn. zm.), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu,	**Dziennik elektroniczny**	NIE (art. 43.1. pkt 4)
6.	Dziennik zajęć przedszkola, oddziału „O” - Przebieg pracy dydaktyczno-wychowawczej z dziećmi w danym roku szkolnym	§ 2.2 rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r. z późn. zm.), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu		NIE (art. 43.1. pkt 4)
7.	Arkusz Ocen - dokumentacja wyników nauczania ucznia w poszczególnych latach	§ 12.1. rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r. z późn. zm.) art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, pesel, nr księgi uczniów, przebieg nauki, wyniki nauki		NIE (art. 43.1. pkt 4)
8.	Ewidencja świadectw szkolnych	§ 5.2 ROZPORZĄDZENIA MINISTRA EDUKACJI NARODOWEJ z dnia 28 maja 2010 r. w sprawie świadectw, dyplomów państwowych i innych druków szkolnych	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, pesel		NIE (art. 43.1. pkt 4)

9.	Ewidencja legitymacji szkolnych	§ 5.2 ROZPORZĄDZENIA MINISTRA EDUKACJI NARODOWEJ z dnia 28 maja 2010 r. w sprawie świadectw, dyplomów państwowych i innych druków szkolnych	Nazwiska, imiona, pesel		NIE (art. 43.1. pkt 4)
10.	Protokoły Rady Pedagogicznej - Protokoły z posiedzenia Rady Pedagogicznej	§ 16 rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r. z późn. zm.) art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.	Nazwiska i imiona, data urodzenia, stan zdrowia		NIE (art. 43.1. pkt 4)
11.	Okręgowa Komisja Egzaminacyjna	Art. 41.1 pkt 1) Rozporządzenia Ministra Edukacji Narodowej z dnia 30 kwietnia 2007 r. w sprawie warunków i sposobu oceniania, klasyfikowania i promowania uczniów i słuchaczy oraz przeprowadzania sprawdzianów i egzaminów w szkołach publicznych (Dz.U. Nr 83 poz.562 z późn. zm.)	Nazwisko, imiona, data i miejsce urodzenia, Pesel, płeć, dysleksja, mniejszość narod.		NIE (art. 43.1. pkt 4)
12.	Stypendia	art. 90f, 90g ustawy z dnia 7 września 1991 r. o systemie oświaty	Imię, nazwisko, data urodzenia, adres zamieszkania, PESEL, NIP, imiona i nazwiska rodziców, adresy zamieszkania, dochody		NIE (art. 43.1. pkt 4)
13.	Wyprawka szkolna	Rozporządzenie Rady Ministrów w sprawie szczegółowych warunków udzielania pomocy finansowej uczniom na zakup podręczników oraz wypłaty uczniom zasiłku powodziowego na cele edukacyjne (Dz.U 2010,nr95, poz.612 z późn. zm)	Nazwisko, imię ucznia, data urodzenia, miejsce urodzenia, adres zamieszkania, imiona i nazwiska rodziców, adres zamieszkania, dochód		NIE (art. 43.1. pkt 4)
14.	Biblioteka	art. 67.1 pkt 2) ustawy z dnia 7 września 1991 r. o systemie oświaty	Nazwisko, imię, adres zam., dane o wypożyczeniach		NIE (art. 43.1. pkt 4) (warunkowo)
15.	Dzienniki Pedagoga i Psychologa - Dziennik zawiera informacje o dzieciach zakwalifikowanych do różnych form pomocy	§ 18 rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r. z późn. zm.), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.	Nazwiska i imiona, Informacje o kontaktach z innymi osobami, instytucjami, stan zdrowia		NIE (art. 43.1. pkt 4)
16.	Dokumentacja Pedagoga i Psychologa oraz logopedy .Dokumentacja badań i czynności uzupełniających prowadzonych przez pedagoga i psychologa	§ 19 rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r. z późn. zm.) art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty	Różne dane niezbędne do dokumentowania przebiegu terapii, nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, stan zdrowia, opinia PPP		NIE (art. 43.1. pkt 4)
17.	Dziennik zajęć rewalidacyjno - wychowawczych Dokumentacja przebiegu zajęć z uczniami upośledzonymi umysłowo.	§ 11 rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z dn. 16 marca 2002 r.), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu		NIE (art. 43.1. pkt 4)
18.	Karty Wycieczek wraz z listą uczestników wycieczek	§ 7.3 pkt 5 rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 8 listopada 2001 r. w sprawie warunków i sposobu organizowania przez publiczne przedszkola, szkoły i placówki krajoznawstwa i turystyki.	Nazwisko i imię, wiek, data urodzenia, adres zamieszkania, PESEL		NIE (art. 43.1. pkt 4)
19.	Dokumentacja wypadków uczniów - Informacje o wypadkach uczniów	§ 43.3 rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 31 grudnia 2002 r. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach.	Nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, stan zdrowia		NIE (art. 43.1. pkt 4)
20.	Karta zapisu dziecka do świetlicy	Rozporządzenie Ministra Edukacji Narodowej z dnia 21 lutego 1994 r. w sprawie rodzajów, organizacji zasad działania publicznych placówek opiekuńczo-wychowawczych i resocjalizacyjnych. (DSz.U. 2007,	Imię (imiona) i nazwisko, datę i miejsce urodzenia oraz adres zamieszkania dziecka, a także imiona i nazwiska rodziców (prawnych opiekunów) oraz		NIE (art. 43.1. pkt 4)

		nr 201,poz.1455 z późn. zm)	adresy ich zamieszkania		
21.	Opinie i Orzeczenia Poradni Psychologiczno-Pedagogicznej	§ 4 ROZPORZĄDZENIEA MINISTRA EDUKACJI NARODOWEJ I SPORTU z dnia 7 stycznia 2003 r. w sprawie zasad udzielania i organizacji pomocy psychologiczno-pedagogicznej w publicznych przedszkolach, szkołach i placówkach (Dz. U. z dnia 29 stycznia 2003 r.)	Imię i nazwisko, data urodzenia, stan zdrowia		NIE (art. 43.1. pkt 4)
22.	Dziennik zajęć pozalekcyjnych	§ 10 Rozporządzenia MENiS z dn. 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji z przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (dz. U. z dn. 16 marca 2002 r. z późn. zm.), art. 22 ust. 2 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty.	Imię i nazwisko, adres zamieszkania		NIE (art. 43.1. pkt 4)
23.	Zgody na przetwarzanie danych	Zgoda osób	Imię i nazwisko adres udzielającego zgodę		NIE (art. 43.1. pkt 4)
24.	Akta osobowe - Zbiór zatrudnionych pracowników	Art. 22 oraz 229 § 7 ustawy z dnia 26.06.1974 Kodeks pracy	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, wykształcenie, przebieg dotychczasowego zatrudnienia, daty urodzenia dzieci, imiona i nazwiska dzieci, stan zdrowia		NIE (art. 43.1. pkt 4)
25.	System Informacji Oświatowej Zbiór zawiera informacje o nauczycielach i uczniach szkoły	Art. 3.4 Ustawy z dnia 19 lutego 2004 r. o systemie informacji oświatowej, Rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 16 grudnia 2004 r. w sprawie szczegółowego zakresu danych w bazach danych oświatowych, zakresu danych identyfikujących podmioty prowadzące bazy danych oświatowych, terminów przekazywania danych między bazami danych oświatowych oraz wzorów wydruków zestawień zbiorczych	PESEL, miejsce pracy, zawód, wykształcenie, wynagrodzenie	SIO	NIE (art. 43.1. pkt 4)
26.	Komisja Socjalna - Świadczenia dla pracowników	Art. 8 ust. 2 ustawy z dnia 4.03.1994 o zakładowym funduszu świadczeń socjalnych	Nazwiska i imiona, adres zamieszkania lub pobytu, stan zdrowia		NIE (art. 43.1. pkt 4)
27.	Dobrowolne ubezpieczenie pracowników	Zgoda osób	Imiona nazwiska, adres zamieszkania lub pobytu, PESEL, nr telefonu		NIE (art. 43.1. pkt 4)
28.	Dokumentacja wypadków pracowników - Informacje o wypadkach pracowników	§ 1.2 rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 19 grudnia 2002 r. (Dz. U. Nr 236, poz. 1992) § 4.1 Rozporządzenia Ministra Gospodarki i Pracy z 16.9.2004 r. w sprawie wzoru protokołu ustalenia okoliczności i przyczyn wypadku przy pracy - Dz. U. Nr 227, poz. 2298	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, NIP, seria i nr dowodu osobistego, stan zdrowia		NIE (art. 43.1. pkt 4)

29.	Umowy zlecenia	Art. 734 – 751 ustawy z dnia 23 kwietnia 1964 r. Kodeks Cywilny (Dz. U. z dnia 18 maja 1964 r.)	Nazwiska i imiona, adres zamieszkania lub pobytu, PESEL, NIP, seria i nr dowodu osobistego, nr telefonu		NIE (art. 43.1. pkt 4)
30.	Przelewy	Ustawa o rachunkowości	Nazwiska, imiona, adresy zamieszkania, nr kont bankowych kontrahentów będących osobami fizycznymi, NIP, wyciągi bankowe	MINIBANK	NIE (art. 43.1. pkt 4) (warunkowo)
31.	Klienci	art. 23.1 pkt 3 ustawy o ochronie danych osobowych	Nazwisko, imię, adres, PESEL, NIP, dowód osobisty		TAK
32.	Faktury	art. 23.1 pkt 3 ustawy o ochronie danych osobowych	Nazwisko, imię, adres zamieszkania	VULCAN	NIE (art. 43.1. pkt 8)
33.	Książka korespondencyjna	Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 1999 r. w sprawie instrukcji kancelaryjnej dla organów gmin i związków międzygminnych (Dz.U. z 1999 r. Nr 112, poz. 1319 z późn.zm.).	Imię i nazwisko, adres zamieszkania		TAK
34.	Ubezpieczenie ZUS - Informacje o pracownikach potrzebne do ubezpieczenia w ZUS	Art. 36.10 oraz art.41.3 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych	Nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, PESEL, NIP	VULCAN	NIE (art. 43.1. pkt 4)
35.	Awans Zawodowy	Art. 9 a, 9 b ust 1 pkt 2ustawy z dnia 26 stycznia 1982 rok Karta Nauczyciela (Dz. U. z 2006 Nr 97 poz. 674 z późn. zm.)	Imiona, nazwisko, nazwisko rodowe, data urodzenia, adres zam. przebieg zatrudnienia, wykształcenie, składniki wynagrodzenia, zapytanie o karalność, stan zdrowia,		NIE (art. 43.1. pkt 4)
36.	Ewidencja zwolnień z w-f	Art8 ust.1 i 2 Rozporządzenia Ministra Wdukacji Narodowej i Sportu z dnia 30 kwietnia 2007r.(Dz.U.2010,nr 156, poz.1046)	Imiona, nazwiska, data urodzenia,		NIE (art. 43.1. pkt 4)

Załącznik nr 2.

EWIDENCJA MIEJSC PRZETWARZNIA DANYCH OSOBOWYCH

Lp.	Nazwa pomieszczenia	Adres	Lokalizacja
1	Sekretariat główny	Ul. Francuska 25 a	Parter
2	Sekretarz szkoły –sekretariat uczniowski	Ul. Francuska 25 a	Parter
3	Sale lekcyjne	Ul. Francuska 25 a Ul. Słowacka 4	Wszystkie kondygnacje
4	Kadry	Ul. Francuska 25a	I piętro Pokój 220
5	Płace	Ul. Francuska 25a	I piętro Pokój 220
6	Kierownik gospodarczy	Ul. Francuska 25a	I piętro Pokój 222
7	Główna księgowa	Ul. Francuska 25a	I piętro Pokój 229
8	Archiwum	Ul. Francuska 25 a	piwnica
9	Pedagog oraz Psycholog	Ul. Francuska 25 a	I piętro , Pokój 223 oraz 224
10.	Biblioteka	Ul. Francuska 25 a	I piętro
11.	Świetlica Gimnazjum	Ul. Francuska 25 a	Parter
12.	Świetlica SP 22	Ul. Słowacka4	Parter

13.	Pokój pedagoga i psychologa	Ul. Słowacka 4	I piętro
14.	Sekretariat	Ul. Słowacka 4	I piętro
15.	Gabinet wicedyrektora	Ul. Słowacka 4	I piętro
16.	Gabinet wicedyrektora	Ul. Francuska 25 a	Parter Pokój 101
17.	Gabinet wicedyrektora	Ul. Francuska 25 a	I piętro Pokój 201
18.	Gabinet wicedyrektora	Ul. Francuska 25 a	II piętro Pokój 301
19.	Pracownia informatyczna	Ul. Francuska 25 a	I piętro Pokój 206
20.	Pracownia informatyczna	Ul. Słowacka 4	Parter Sala nr 5
21.	Pokój nauczycielski SP	Ul. Słowacka 4	I Piętro

Załącznik nr 3.

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Nazwisko, Imię	Nr zbiorów	Nr upoważnienia
1	Monika Marciniak	23,33,36	1-2010
2	Magdalena Janicka	2,3,4,7,8,9,25	2-2010
3	Agnieszka Romańczuk - Karwicka	24,25,26,30,35, 36	3-210
4	Renata Szczepaniak	25,27,28,29,30, 34.	4-2010
5	Wanda Josicz	26,30, 31, 32,34	5-2010
6	Katarzyna Żarczyńska	26,30, 31, 32,34	6-2010
7	Izabela Kubiak	31,32	7-2010
8	Bogumiła Łęczycka	30, 31, 32,34	8-2010
9	Jadwiga Siedlecka	1,3,4,7,8,9,	9-2010
10	Małgorzata Harasymowicz	5,12,13,15,16,17	10-2010
11	Magdalena Kamińska	5,15,16,17,21	11-2010
12	Anna Kwilman	10,14	12-2010
13	Anna Najman	5,14	13-2010
14	Katarzyna Oleńska	5,14	14-2010

15	Małgorzata Szmytkiewicz	5,12,13,15,16,17	15-2010
16	Marzenna Hozakowska	3,5,11,17,18,21,22, 35	16-2010
17	Teresa Konieczka	3,5,11,14,17,18,21, 22,35	17-2010
18	Mariusz Szpakowicz	3,5,17,18,	18-2010
19	Urszula Broda	11,17,22,35	19-2010
20	Adler Mirosława	5,17	20-2010
21	Błaszczyk Elżbieta	5	21-2010
22	Bobrek-Worchacz Magdalena	5	22-2010
23	Broda Urszula	5	23-2010
24	Broda-Karłyk Anna	5	24-2010
25	Brosławska Mariola	5	25-2010
26	Bryńska Jolanta	5,19	26-2010
27	Brzóska Grażyna	5	27-2010
28	Buczacka Iwona	5	28-2010
29	Ceglarska Monika	5,16	29-2010
30	Chalecka Marlena	5,20	30-2010
31	Chinalska Krystyna	5	31-2010
32	Chojak Maria	5	32-2010
33	Chumas Joanna	5	33-2010

34	Czerwonogrodzka Maja	5	34-2010
35	Dąbrowska Beata	5	35-2010
36	Felińska Edyta	5,20,	36-2010
37	Franek Piotr	5	37-2010
38	Frankiewicz Diana	5,17	38-2010
39	Frodyma Roman	5	39-2010
40	Gadomska Anna	5	40-2010
41	Galus Magdalena	5,17	41-2010
42	Gorzelana Joanna	5	42-2010
43	Gorzelany Rafał	5	43-2010
44	Grabska Anna	5	44-2010
45	Graczykowska-Lindenberg Renata	5,17	45-2010
46	Grupa Cecylia	5	46-2010
47	Grzesiak Jerzy	5	47-2010
48	Harla Jolanta	5,17	48-2010
49	Hassa Adela	5	49-2010
50	Heba Katarzyna	5	50-2010
51	Horanin Małgorzata	5,17	51-2010
52	Jabłońska Anna	5	52-2010

53	Jagusiak Jolanta	5,17	53-2010
54	Jakubowska Magdalena	5	54-2010
55	Janik Wioletta	5	55-2010
56	Jażdżewska-Drobek Joanna	5,17	56-2010
57	Juny-Pilarska Katarzyna	5	57-2010
58	Jurkiewicz Alicja	5,17	58-2010
59	Jurkiewicz Edyta	5	59-2010
60	Kaczmarek Magdalena	5,17	60-2010
61	Kaczmarek Radosław	5	61-2010
62	Kaczmarek Wioletta	5	62-2010
63	Kapalska Grażyna	5	63-2010
64	Kaszubska Agnieszka	5,17	64-2010
65	Kociemba-Trąbka Małgorzata	5	65-2010
66	Kolman-Zatorska Anna	5	66-2010
67	Kołodziejska Beata	5	67-2010
68	Korbanek Agnieszka	5,20	68-2010
69	Korzeniowska Małgorzata	5,16	69-2010
70	Kowal Eugeniusz	5	70-2010
71	Krengowska Jagna	5	71-2010

72	Krystians Grzegorz	5	72-2010
73	Krzesińska Magdalena	5,17	73-2010
74	Ksepko Piotr	5,17	74-2010
75	Kucharczyk Arleta	5,16	75-2010
76	Kucofaj-Turok Katarzyna	5,20	76-2010
77	Kumanowska Marzena	5,17	77-2010
78	Kutnik Ireneusz	5	78-2010
79	Kutnik Lidia	5	79-2010
80	Kwilman Anna	5	80-2010
81	Laskowska Agnieszka	5	81-2010
82	Liwocha Bogusława	5,17	82-2010
83	Majorczyk Hanna	5,6,17	83-2010
84	Małachowska Katarzyna	5,17	84-2010
85	Michalczuk Joanna	5	85-2010
86	Mikunda Irena	5	86-2010
87	Mleczko Elżbieta	5	87-2010
88	Modrzyk Małgorzata	5	88-2010
89	Najder Włodzimierz	5,17	89-2010
90	Nakoneczna-Kupnicka Joanna	5	90-2010

91	Niedziela Agata	5	91-2010
92	Nowak Agnieszka	5,17	92-2010
93	Nowak Jolanta	5	93-2010
94	Nowicka Daria	5,17	94-2010
95	Olszewska Kalina	5	95-2010
96	Oniszczuk Anna	5	96-2010
97	Petryków Piotr	5	97-2010
98	Pszonka Elżbieta	5	98-2010
99	Rozestwińska Agnieszka	5	99-2010
100	Rządzka Mirosława	5,16	100-2010
101	Rzemieniecka Anetta	5	101-2010
102	Sawicka Elwira	5,3	102-2010
103	Schwickert Jolanta	5	103-2010
104	Semkło Anna	5,6	104-2010
105	Sieczkowska Agnieszka	5,17	105-2010
106	Sienkiewicz Aneta	5	106-2010
107	Sitek Aneta	5	107-2010
108	Solarek Jan	5	108-2010
109	Sprawka Jolanta	5	109-2010

110	Stachowiak Agata	5,17	110-2010
111	Stachowska Anna	5	111-2010
112	Stankiewicz Dorota	5,17	112-2010
113	Strzelec-Solarek Danuta	5	113-2010
114	Suchodolska Ewa	5	114-2010
115	Sznajder Małgorzata	5,17	115-2010
116	Szpak Joanna	5	116-2010
117	Szurowska Joanna	5	117-2010
118	Śliwińska Małgorzata	5	118-2010
119	Topczewska Adriana	5	119-2010
120	Truszkiewicz Danuta	5,17	120-2010
121	Tyliszczak Małgorzata	5	121-2010
122	Tyliszczak Sławomir	5	122-2010
123	Tyszer Jolanta	5	123-2010
124	Ufa Gabriela	5	124-2010
125	Wejdelek-Zembrzuska Justyna	5	125-2010
126	Wierzchowiecka Lidia	5	126-2010
127	Worchacz Damian	5	127-2010
128	Zaranowski Artur	5	128-2010

129	Zawada Tomasz	5	129-2010
130	Zielińska Iwona	5	130-2010
131	Zieniewicz Marzena	5	131-2010
132	Zuber Cecylia	5	132-2010
133	Zubowicz-Jaszcza Elżbieta	5	133-2010
134	Żyto Piotr	5,17	134-2010
135	Ireneusz Bućko	28	135-2010
136	Andrzej Jakubiak	5,17	1-2011

Załącznik nr 4.

……., dn. …….

-2010

…….

(sygnatura)

WAŻNOŚĆ
od: ……
do: ***do ustania zatrudnienia lub odwołania***

UPOWAŻNIENIE

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101 poz. 926, ze zm.) upoważniam Panią/Pana:

……

do przetwarzania, w ramach wykonywanych obowiązków służbowych, następujących zbiorów danych osobowych:

Nr zbiorów z ewidencji zbiorów

……

(podpis ADO)

Załącznik nr 5.

……., dn. ……

……

(sygnatura)

UNIEWAŻNIENIE

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101 poz. 926, ze zm.) unieważniam upoważnienie do przetwarzania danych osobowych wydane dnia …….. o sygnaturze ……. dla Pani/Pana:

……

……

(podpis ADO)

Załącznik nr 6.

……, dn. ……

……

……

(imię i nazwisko pracownika)

OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana mi jest treść:

   a) Dokumentacji ochrony danych osobowych w Zespole Szkół Ekologicznych im. Unii Europejskiej w Zielonej Górze,
   b) Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926),
   c) Rozporządzenie 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).

2. Jednocześnie zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/zapoznałam się z racji wykonywanej pracy, a w szczególności nie będę:

   a) ujawniać danych zawartych w eksploatowanych w systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
   b) ujawniać szczegółów technologicznych używanych w systemów oraz oprogramowania,
   c) udostępniać osobom nieupoważnionym nośników magnetycznych i optycznych oraz wydruków komputerowych,
   d) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą Dokumentacją.

…….. ……

(podpis pracownika) (podpis przełożonego)

Załącznik nr 7.

……, dn. ……

……

(sygnatura)

WAŻNOŚĆ
od: ……
do: *ustania zatrudnienia bądź odwołania*

ZGODA

NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH

Na podstawie pkt I.2 załącznika do Rozporządzenia 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 z późn. zm.), **wyrażam zgodę Pani/Panu:**

……

na przebywanie w pomieszczeniach, w których przetwarzane są dane osobowe w zakresie niezbędnym do wykonywania obowiązków służbowych.

……
(podpis ADO)

Załącznik nr 8.

……., dn. ……

……

(sygnatura)

ODWOŁANIE ZGODY

NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH

Na podstawie pkt I.2 załącznika do Rozporządzenia 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 z późn. zm.), **odwołuję zgodę** z dnia ……o sygnaturze …… udzieloną **Pani/Panu:**

…….

do przebywania w pomieszczeniach, w których przetwarzane są dane osobowe.

……

(podpis ADO)

Załącznik nr 9.

RAPORT
z naruszenia bezpieczeństwa zasad ochrony danych osobowych
w Zespole Szkół Ekologicznych im. Unii Europejskiej w Zielonej Górze

1. Data: ……. …… Godzina: ……
(dd.mm.rr) (gg:mm)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

……..
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:

……..
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
……..
……..
……..

5. Przyczyny wystąpienia zdarzenia:
……..
……..
……..

6. Podjęte działania:
……..
……..
……..

7. Postępowanie wyjaśniające:
……..
……..
……..

……..
(data, podpis ADO)

Załącznik nr 10.

Zielona Góra, dnia .....

Powołanie Administratora

Bezpieczeństwa Informacji

1. Na podstawie art. 36 ust. 3 ustawy dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) z dniem …….. 2010 r. ***wyznaczam***

Pana/Panią .....

zam. …… legitymującą się dowodem osobistym

nr .....wydanym przez ……..

na Administratora Bezpieczeństwa Informacji.

1. Do obowiązków ABI należy:

- Nadzór nad przetwarzaniem danych zgodnie z ustawą o ochronie danych osobowych i innymi przepisami prawa.
- Kontrola przestrzegania zasad ochrony – systematycznie, nie rzadziej niż dwa razy do roku kontrolowanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności kontrola pod kątem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, w szczególności:
    - Kontrola dokumentacji opisującej sposób przetwarzania oraz ochrony.
    - Kontrola fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są informacje.
    - Kontrola poprawności zabezpieczeń danych przetwarzanych metodami tradycyjnymi.
    - Kontrola awaryjnego zasilania komputerów.
    - Nadzór nad naprawą, konserwacją oraz likwidacją urządzeń komputerowych.

- Kontrola systemu kontroli obecności wirusów komputerowych.
- Kontrola wykonywania kopii awaryjnych.
- Kontrola przeglądu, konserwacji oraz uaktualnienia systemów informatycznych.
- Kontrola mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych.
- Kontrola nadanych upoważnień.

- Przedstawianie Administratorowi danych wyników kontroli.
- Systematyczna analiza dokumentacji pod kątem obszarów, zbiorów oraz zasad ochrony.
- Podjęcie natychmiastowych działań zabezpieczających w przypadku otrzymania informacji o naruszeniu bezpieczeństwa informacji. Zagrożenie bezpieczeństwa opisano formy naruszenia zbiorów i tryb dalszego postępowania opisano w zał. nr 12 do Polityki Bezpieczeństwa w Zespole Szkół Ekologicznych im. Unii Europejskiej w Zielonej Górze
- Prowadzenie monitoringu przetwarzania danych.
- Każdorazowe sporządzenie raportu zgodnie ze wzorem będącym załącznikiem nr 9 do Polityki Bezpieczeństwa w Zespole Szkół Ekologicznych im. Unii Europejskiej w Zielonej Górze oraz przedstawienie efektów działań Administratorowi danych.

....

podpis (podpis dyrektora)

Administratora Bezpieczeństwa Informacji

Załącznik nr 11.

……, dn. ……

……

……
(imię i nazwisko, adres zamieszkania)

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Na podstawie art. 23 ust.1 pkt 1 (oraz/lub art. 27.2 pkt 1 – dla danych wrażliwych) ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926), wyrażam zgodę na przetwarzanie niżej wymienionych moich danych osobowych.

Zgoda udzielona jest tylko do przetwarzania danych oraz ich udostępniania w podanym niżej zakresie.

Lp.	Zakres danych – zgoda	Cel przetwarzania
1	Zgoda na przetwarzanie wizerunku dziecka	Prowadzenie strony internetowej oraz publikacje związane z działalnością szkoły
2	Dane osobowe dziecka	Prowadzenie dokumentacji szkolnej dziecka zgodnie z obowiązującym prawem.

Jednocześnie zgodnie z art. 24 ust. 1 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926) przyjmuję do wiadomości, że:

- Administratorem danych jest Zespół Szkół Ekologicznych im. Unii Europejskiej z siedzibą w Zielonej Górze przy ul. Francuskiej 25a,
- dane będą przetwarzane wyłączenie zgodnie z określonym celem,
- dane będą udostępniane wyłącznie w uzasadnionych prawnie celach,
- przysługuje mi prawo dostępu do treści danych oraz ich poprawiania,
- dane podaję dobrowolnie.

……

Podpis Rodzica /Opiekuna

Załącznik nr 12.

ZAGROŻENIA BEZPIECZEŃSTWA

I. Charakterystyka możliwych zagrożeń

- **Zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, a ciągłość systemu zostaje zakłócona lecz nie dochodzi do naruszenia poufności danych.
- **zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia danych, a ciągłość pracy systemu może zostać zakłócona oraz może nastąpić naruszenie poufności danych,
- **zagrożenia zamierzone, świadome i celowe** - najpoważniejsze zagrożenia, gdzie występuje naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie 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.

II. Sytuacje świadczące o naruszeniu zasad bezpieczeństwa

- **Przełamane zabezpieczenia tradycyjnych** – zerwane plomby na drzwiach, szafach, segregatorach,
- **sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych** na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
- **niewłaściwe parametry środowiska**, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
- **awaria sprzętu lub oprogramowania**, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
- **pojawienie się odpowiedniego komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,

- **jakość danych w systemie** lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
- **naruszenie lub próba naruszenia integralności** systemu lub bazy danych w tym systemie,
- **próba lub modyfikacja danych** oraz zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
- **niedopuszczalna manipulacja** danymi osobowymi w systemie,
- **ujawnienie osobom nieupoważnionym** danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu,
- **praca w systemie lub jego sieci komputerowej wykazująca nieprzypadkowe odstępstwa** od założonego rytmu pracy oraz wskazująca na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
- **ujawnienie istnienia nieautoryzowanych kont dostępu** do danych lub tzw. „bocznej furtki", itp.,
- **podmiana lub zniszczenie nośników z danymi osobowymi** bez odpowiedniego upoważnienia lub w sposób niedozwolony kasowania lub kopiowanie danych,
- **rażące naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji** (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

III. Tabele form naruszenia bezpieczeństwa i sposoby postępowania

Tabela form naruszenia ochrony danych osobowych przez osoby zatrudnione przy przetwarzaniu danych

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
W ZAKRESIE WIEDZY	
Ujawnianie sposobu działania aplikacji i systemu oraz 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.
Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	
Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji.	
W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA	
Opuszczenie stanowiska pracy i pozostawienie	Niezwłocznie zakończyć działanie aplikacji.

aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Sporządzić raport
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.
Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych osobom nieuprawnionym.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Sporządzić raport.
Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymieniona czynność, aby jej zaniechała. Sporządzić raport.
Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność o szkodliwości takiego działania. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport.
W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE	
Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Sporządzić raport.
Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń. Sporządzić raport.
Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport.
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
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.

Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	
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 pomieszczenie. Powiadomić przełożonych. Sporządzić raport.
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 administratora bezpieczeństwa informacji. Sporządzić raport.
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 czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i administratora bezpieczeństwa informacji. Sporządzić raport.
W ZAKRESIE POMIESZCZEŃ W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI	
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 czynność do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i administratora bezpieczeństwa informacji. Sporządzić raport.
Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i administratora bezpieczeństwa informacji. Sporządzić raport.

Tabela zjawisk świadczących o możliwości naruszenia ochrony danych osobowych

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
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.
Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	
Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.	
Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	
Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie administratora bezpieczeństwa informacji. Sporządzić raport.

Tabela naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	Powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	

Złącznik nr 13

Zielona Góra, dnia .....

Powołanie Administratora

Systemu Informatycznego

1. Na podstawie art. 36 ust. 3 ustawy dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) z dniem ……. 2010 r. ***wyznaczam***

Pana/Panią .....

zam. …… legitymującą się dowodem osobistym nr .....wydanym przez …….……..

na Administratora Systemu Informatycznego (ASI).

ASI odpowiada za korygowanie instrukcji zarządzania informatycznego w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych sieci teleinformatycznej.

Polityka Bezpieczeństwa w Zespole Szkół Ekologicznych im. Unii Europejskiej w Zielonej Górze zawiera -47- stron.

Sporządził: Administrator Bezpieczeństwa Informacji

ZATWIERDZAM:

Data: .....

Administrator Danych Osobowych

.....

(podpis i pieczęć)