POLITYKA BEZPIECZEŃSTWA

PUBLICZNEGO GIMNAZJUM
W CZAŃCU
IM. KARDYNAŁA KAROLA WOJTYŁY

Zakres przedmiotowy procedury:

Stan prawny

I. Definicje.
II. Cele i założenia.
III. Wykaz budynków i pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe.
IV. Zakres stosowania.
V. Infrastruktura przetwarzania danych.
VI. Organizacja przetwarzania danych osobowych - zakresy czynności.
VII. Postępowanie w przypadku w przypadku naruszenia zasad przetwarzania danych osobowych.
VIII. Poziom bezpieczeństwa.
IX. Środki techniczne i organizacyjne zabezpieczające.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

- Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
- Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 roku;
- Ustawą o systemie oświaty z dnia 7 września 1991 roku;
- Ustawą o systemie informacji oświatowej z dni 16 grudnia 2004;
- Rozporządzeniem Ministra Edukacji Narodowej i Sportu w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu

nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji z dnia 19 lutego 2002 r.

I. DEFINICJE.

1. **Dane osobowe** - są to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Informacje mogą przybierać różne formy. Może być ona zapisywana lub wydrukowana na papierze, przechowywana elektronicznie, przesyłana pocztą lub za pomocą urządzeń elektronicznych, wypowiadana ustnie.
2. **Zbiór danych** - 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.
3. **Przetwarzanie 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.

   Informacja ma dla Szkoły wartość i dlatego należy zapewnić jej bezpieczeństwo. Bezpieczeństwo informacji oznacza ochronę przed wieloma różnymi zagrożeniami, aby zapewnić prawidłową działalność szkoły.
4. **Sieci publiczne** – rozumie się przez to publiczną sieć telekomunikacyjna w rozumieniu art. 2 pkt. 29 ustawy z 16 lipca 2004 Prawo Telekomunikacyjne.
5. **Hasło –** rozumie się przez to ciąg znaków literowych, cyfrowych lub innych znanych jedynie osobie uprawnionej do pracy w systemie informatycznym.
6. **Identyfikator** – rozumie się przez to ciąg znaków literowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

7. **Użytkownik** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.
8. **Osoba upoważniona –** rozumie się przez to osobę upoważnioną do przetwarzaniach danych osobowych, która została upoważniona na piśmie.
9. **Osoba nieupoważniona** – rozumie się przez to osobę która nie jest upoważniona w ogóle lub w danym zakresie do przetwarzania danych osobowych.

II. CELE I ZAŁOŻENIA

Oświadczenie Dyrektora Szkoły:

Jestem świadomy wartości informacji Szkoły.

Spełnienie wymagań prawnych jest celem podstawowym.

Chroniąc informacje zachowujemy prywatność i godność każdego obywatela oraz dbamy o interesy dzieci i uczniów i ich rodziców.

Uczymy się i wyciągamy wnioski z błędów.

Obowiązkiem pracowników jest przestrzeganie szczegółowych zasad postępowania, a w szczególności zasady: „co nie jest dozwolone jest zabronione".

Celem polityki jest wskazanie działań jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki w zakresie bezpieczeństwa danych.

Dla spełnienia wymagań dotyczących zarządzania bezpieczeństwem informacji konieczny jest aktywny udział wszystkich pracowników. Każdy pracownik zobligowany jest do zapoznania się z dokumentem polityki bezpieczeństwa i bezwzględnego przestrzegania zasad w nim zawartych.

Polityka bezpieczeństwa ochrony zbiorów danych osobowych sformułowana została w oparciu o zasady zachowania poufności, integralności i dostępności informacji.

- Poufność - zapewnienie, że informacja jest dostępna jedynie osobom upoważnionym;
- Integralność - zapewnienie dokładności i kompletności informacji oraz metod przetwarzania;
- Dostępność - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne

III. WYKAZ BUDYNKÓW I POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE.

Dane osobowe przetwarzane są w budynku przy ul. Kardynała Karola Wojtyły 119 w Czańcu, Regon: 072327469 w następujących pomieszczeniach:

- Gabinet Dyrektora
- Sekretariat
- Pokój nauczycielski
- Biblioteka
- Pokój Pedagoga
- Gabinet Higienistki.

IV. ZAKRES STOSOWANIA.

Polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny jak i w systemach informatycznych. Procedury i zasady określone w niniejszym dokumencie stosuję się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych jak i innych, np. zleceniobiorców, praktykantów, stażystów.

V. INFRASTRUKTURA PRZETWARZANIA DANYCH OSOBOWYCH.

1. Wykaz zbiorów danych osobowych – w załączeniu.
2. Sposób przepływu informacji

   Programy wykorzystywane nie wymagają wymiany danych, w związku z powyższym nie ma przepływu danych.

VI. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH – ZAKRES CZYNNOŚCI:

Administrator Danych Osobowych w szczególności:

- upoważnia poszczególne osoby do przetwarzania danych osobowych w stosownym zakresie;
- wyznacza administratora bezpieczeństwa informacji i ustala zakres jego czynności;
- podejmuje odpowiednie czynności w przypadku naruszenia procedur bezpieczeństwa przetwarzania danych;
- podejmuje decyzje o celach i środkach przetwarzania danych osobowych;

- sprawuje nadzór nad wdrożeniem środków organizacyjnych, technicznych i fizycznych w celu zabezpieczenia danych;

Administrator Bezpieczeństwa Informacji w szczególności:

- prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych;
- prowadzi dokumentacje normującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę danych osobowych
- przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych;
- podejmuje stosowane działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego;
- w porozumieniu z Administratorem Danych Osobowych na czas swojego urlopu wyznacza zastępcę.

Administrator Systemu Informatycznego w szczególności:

- zarządza systemem informatycznym, w którym są przetwarzane dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;
- przeciwdziała dostępowi osób niepowołanych do systemu informatycznego w którym są przetwarzane dane osobowe;
- przydziela każdemu użytkownikowi identyfikator i hasło do systemu informatycznego w ramach upoważnienia do przetwarzania danych osobowych – dokonuje również na wniosek ewentualnych modyfikacji uprawnień;
- nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;

- ASI wyrejestrowuje użytkowników na polecenie administratora danych;

Osoba upoważniona do przetwarzania danych osobowych:

- może przetwarzać dane osobowe: wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych Osobowych (upoważnienia pisemne – w załączeniu) i tylko w celu wykonywania nałożonych na niego obowiązków.
- ma dostęp do danych osobowych - przypisany jest do **niepowtarzalnego identyfikatora użytkownika** co oznacza, że użytkownik nie udostępnia swojego identyfikatora i hasła współpracownikom i nie rozpowszechnia go poprzez przyklejanie go na tablicach, monitorach czy innych miejscach.
- Zobowiązana jest do zachowanie tajemnicy - użytkownicy danych pisemnie oświadczają (klauzula zawarta w upoważnieniu), że zobowiązują się do zachowania tajemnicy danych osobowych oraz przestrzegania procedur ich bezpiecznego przetwarzania - przestrzeganie tajemnicy obowiązuje przez cały okres zatrudnienia, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji.

Wygaśniecie upoważnienia do przetwarzania danych spowodowane jest poprzez rozwiązania stosunku pracy lub odwołanie z pełnionej funkcji.

Naruszenie procedur bezpieczeństwa przetwarzania danych osobowych, w szczególności polegające na świadomym udostępnieniu danych osobie niepowołanej –- jest ciężkim naruszeniem obowiązków pracowniczych i może być uzasadnieniem rozwiązania umowy o pracę bez wypowiedzenia.

Wszyscy użytkownicy zobowiązani są do zapoznania się z przepisami prawa w zakresie danych osobowych w tym z przepisami polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym;

VII. POSTĘPOWANIE W PRZYPADKU NARUSZENIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH.

1. Każde zdarzenie wskazujące na naruszenie zasad ochrony danych osobowych przyjęte jako obowiązujące - zgodnie z ustawą o ochronie danych osobowych, mające wpływ na:
   1) stan urządzeń; system zabezpieczeń obiektu; stan aktywnych urządzeń sieciowych i pozostałej infrastruktury informatycznej; zawartość zbioru danych; ujawnione metody pracy; sposób działania programu; jakość komunikacji w sieci telekomunikacyjnej;
   2) przebywanie osób nieuprawnionych wewnątrz obszaru przetwarzania danych osobowych; inne zdarzenia mogące mieć wpływ na naruszenie systemu informatycznego w tym obecność wirusów; stanowi dla każdej osoby uprawnionej do przetwarzania danych osobowych, podstawę do natychmiastowego reagowania według poniższych zaleceń :
      - zabezpieczenia miejsca zdarzenia w sposób uniemożliwiający dalsze korzystanie ze zbiorów danych osobowych i uniemożliwiający zmianę stanu faktycznego,
      - niezwłocznego powiadomienia ADO, ABI i ASI,
      - oczekiwania w miejscu zdarzenia na Administratora Bezpieczeństwa Informacji lub inną osobę upoważnioną przez Administratora Danych Osobowych,
      - udzielania wyjaśnień dotyczących zdarzenia. Osoba stwierdzająca naruszenie przepisów lub stan mogący mieć wpływ na bezpieczeństwo zobowiązana jest do możliwie pełnego udokumentowania zdarzenia celem precyzyjnego określenia przyczyn i ewentualnych skutków naruszenia obowiązujących zasad.

Powyższy wykaz zdarzeń nie jest katalogiem zamkniętym.

Administrator Bezpieczeństwa Informacji lub inna osoba wskazana przez Administratora Danych Osobowych zabezpiecza miejsce zdarzenia w celu zabezpieczenia danych osobowych jak również dowodów mających wpływ na określenie naruszenia ochrony danych.

W razie konieczności wyjaśnienia faktów określonych w pkt. 1 Administrator powołuje komisję, w skład której wchodzi Administrator Bezpieczeństwa Informacji, osoba odpowiedzialna za organizację pracy na danym odcinku oraz Administratora Systemu Informatycznego, ponadto w ustaleniach uczestniczy osoba kierująca obszarem w którym doszło do naruszenia.

Komisja ma na celu ustalenie:

- czy doszło do naruszenia ochrony danych osobowych,
- jeżeli doszło do naruszenia ochrony to określić jego stopień,
- osoby odpowiedzialnej za uchybienia,
- środków zapobiegawczych i naprawczych.

Ustalenia komisji w formie protokołu przekazywane są do Administratora Danych Osobowych (wzór w załączeniu).

W przypadku kradzieży lub zaginięcia sprzętu służącego do przetwarzania danych osobowych należy niezwłocznie powiadomić ADO, ABI I ASI.

VIII. POZIOM BEZPIECZEŃSTWA.

Z uwagi na fakt połączenia urządzeń systemu informatycznego z siecią publiczną (Internet) zgodnie z paragrafem 6 ust. 4 rozporządzenia MSWiA zapewnia się **wysoki poziom bezpieczeństwa** przetwarzania danych osobowych w systemie informatycznym.

IX. ŚRODKI TECHNICZNE I ORGANIZACYJNE ZABEZPIECZAJĄCE.

1. Do przetwarzania danych dopuszczone są wyłącznie osoby posiadające upoważnienie, nadane przez Administratora Danych Osobowych. Wykaz osób upoważnionych do przetwarzania danych osobowych prowadzi ABI.
2. Do obsługi systemów informatycznych i urządzeń wchodzących w ich skład, dopuszczone są wyłącznie osoby posiadające upoważnienie, nadane przez Administratora Danych Osobowych. Każda z tych osób posiada indywidualny identyfikator i hasło. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych nie może być przydzielony innej osobie.
3. Podczas nieobecności upoważnionych pracowników do przetwarzania danych, miejsca wyznaczone do przetwarzania tych danych są zamykane lub zabezpieczane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.
4. Osoby trzecie, które świadczą usługi na rzecz szkoły, mogą mieć dostęp do wyznaczonych pomieszczeń tylko wówczas jeżeli posiadają odpowiednie zezwolenie lub na podstawie umowy o świadczenie usług (firmy ochroniarskie, remontowe).

   Dane osób wykonujących powyższe czynności znajdują się u Dyrektora.
5. Ekrany komputerów w których przetwarzane są dane osobowe umieszczone są w sposób uniemożliwiający obserwację przetwarzania danych przez osoby postronne.
6. Dokumenty papierowe i nośniki komputerowe kiedy nie są używane, a szczególnie poza godzinami pracy należy przechowywać w odpowiednich, zamykanych szafach lub innego rodzaju zabezpieczanych meblach.

7. Każdy dokument, zawierający dane osobowe lub inne dane umożliwiające identyfikację osób, po ustaniu jego użyteczności, niezwłocznie niszczy się w niszczarce do papieru.
8. Osoby używające komputerów przenośnych zawierających dane osobowe zachowują szczególną ostrożność podczas ich transportu, przechowywania i użytkowania.
9. Zabrania się wynoszenia poza teren sprzętu, informacji i oprogramowania bez zezwolenia.
10. Zabrania się powtórnego używania jednostronnie zadrukowanych dokumentów.
11. Wydruki z programów zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobą postronnym.
12. Zabrania się zapisywania hasła wymaganego do uwierzytelnienia w systemie na papierze lub innych nośnikach.
13. Zastosowano fizyczne zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe: system alarmowy i przeciwpożarowy, szyby antywłamaniowe w pokoju nauczycielskim i kancelarii.
14. Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej zapewniają zasilacze UPS.
15. Zbiory papierowe znajdują się w szafach zamykanych na zamki. W sekretariacie i kancelarii sprawy kadrowe przechowywane są w szafie metalowej.
16. Budynek szkoły, w którym przetwarzane są dane osobowe wyposażone są w system alarmowy przeciwłamaniowy.
17. Budynek szkoły, w którym są przetwarzane dane osobowe są zabezpieczone przed pożarami za pomocą wolnostojących gaśnic.
18. Kopie zapasowe zbioru danych osobowych są przechowywane w innym pomieszczeniu, niż to w którym się znajduje komputer główny, na którym dane osobowe są przetwarzane na bieżąco.
19. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora

użytkownika oraz hasła - niemożliwe jest załogowanie się do systemu jako anonimowy użytkownik.

20. Zastosowano okresowe zmiany haseł.
21. Zastosowano mechanizm umożliwiający rejestrację identyfikatora użytkownika wprowadzającego dane osobowe.
22. Urządzenia, dyski lub inne nośniki informacji zawierające dane osobowe przeznaczone do:
    - likwidacji - pozbawia się wcześniej zapisu tych danych a jeśli to nie jest to nie możliwe uszkadza się w sposób uniemożliwiający ich odczytanie;
    - przekazania: pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie;
    - naprawy: pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie lub naprawia się je pod nadzorem osoby upoważnionej przez ADO.
23. System informatyczny służący do przetwarzania danych osobowych chroni przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.