POLITYKA OCHRONY DANYCH OSOBOWYCH

w Zespole Szkół Chemiczno-Elektronicznych im. Jana Pawła II w Inowrocławiu

aktualizacja

Inowrocław, październik 2021 r.

Spis treści

Zespół Szkół Chemiczno-Elektronicznych im. Jana Pawła II w Inowrocławiu

I. POSTANOWIENIA OGÓLNE

§1.

1. Celem Polityki ochrony danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania w Zespole Szkół Chemiczno-Elektronicznych im. Jana Pawła II w Inowrocławiu grupy informacji zawierającej dane osobowe.

§2.

I. Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1. szkoła – Zespół Szkół Chemiczno-Elektronicznych im. Jana Pawła II w Inowrocławiu
2. dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3. przetwarzanie danych osobowych – gromadzenie, utrwalanie przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych,
4. użytkownik – osoba upoważniona do przetwarzania danych osobowych,
5. administrator szkolnej sieci komputerowej – osoba upoważniona do zarządzania systemem informatycznym,
6. system informatyczny – system przetwarzania danych w Zespole Szkół Chemiczno-Elektronicznych im. Jana Pawła II w Inowrocławiu wraz z zasobami ludzkimi, technicznymi oraz finansowymi, który dostarcza i rozprowadza informacje,
7. zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.

II. DEFINICJA BEZPIECZEŃSTWA INFORMACJI

§3.

1. Utrzymanie bezpieczeństwa przetwarzanych przez szkolę informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.
2. Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:
   1) Poufność informacji – rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,
   2) Integralność informacji – rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
   3) Dostępność informacji – rozumiane jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
   4) Zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.
3. Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:
   1) Niezaprzeczalności odbioru – rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie,
   2) Niezaprzeczalności nadania – rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie,
   3) Rozliczalności działań – rozumianej, jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał.

III. ZAKRES

§4.

1. W systemie informacyjnym szkoły przetwarzane są informacje służące do wykonywania zadań niezbędnych dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa.
2. Informacje te są przetwarzane i składowane zarówno w postaci manualnej jak i elektronicznej.

§5.

I. Politykę Bezpieczeństwa stosuje się do:

1. danych osobowych przetwarzanych w systemie informatycznym,
2. wszystkich informacji dotyczących danych pracowników szkoły, w tym danych osobowych personelu i treści zawieranych umów o pracę,
3. wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji,
4. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
5. rejestru osób dopuszczonych do przetwarzania danych osobowych,
6. innych dokumentów zawierających dane osobowe.

§6.

I. Zakresy określone przez dokumenty Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego szkoły w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie,
2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
3) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

1. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy oraz inne osoby mające dostęp do informacji podlegających ochronie.

§7.

1. Informacje niejawne nie są objęte zakresem niniejszej Polityki.

IV. STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA INFORMACJI

§8.

1. Dokumenty Polityki Bezpieczeństwa Informacji ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.
2. Zestaw dokumentów Polityki Bezpieczeństwa Informacji składa się z:
   1) Niniejszego dokumentu Polityki Bezpieczeństwa Informacji,
   2) Instrukcji zarządzania systemem informatycznym w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych, opisującej sposób zarządzania systemami przetwarzania danych osobowych w szkole.

V. DOSTĘP DO INFORMACJI

§9.

1. Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w szkole zasad ochrony danych osobowych.

§10.

1. Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

§11.

1. Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa jest możliwe, jeżeli podmioty te w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

§12.

1. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§13.

1.Dane osobowe udostępnia się na pisemny, umotywowany wniosek, który powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać zakres i przeznaczenie.

VI.ZARZĄDZANIE DANYMI OSOBOWYMI

§14.

1. Administratorem danych osobowych jest Zespół Szkół Chemiczno-Elektronicznych im. Jana Pawła II w Inowrocławiu., w imieniu którego działa dyrektor szkoły Dorota Gliwińska.

§15.

1. Za bezpieczeństwo danych osobowych Jednostki, odpowiada:

Administrator danych osobowych – Zespół Szkół Chemiczno-Elektronicznych im. Jana Pawła II w Inowrocławiu,

2. W umowach zawieranych przez szkołę winny znajdować się postanowienia zobowiązujące podmioty zewnętrzne do ochrony danych udostępnionych przez szkołę.

§16.

1. Ochrona zasobów danych osobowych szkoły jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników szkoły .

VII. ZAKRESY ODPOWIEDZIALNOŚCI

§18.

1. Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik szkoły.

§19.

I. Administrator szkolnej sieci komputerowej w szkole:
   1. odpowiada za realizację ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora Bezpieczeństwa Informacji,
   2. sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób,
   3. określa strategię zabezpieczania systemów informatycznych szkoły,
   4. sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
   5. sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe,

6. identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych szkoły,
7. określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
8. sprawuje nadzór nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, palmtopach, w których przetwarzane są dane osobowe,
9. sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe,
10. monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,
11. sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych,
12. zatwierdza wnioski o przyznaniu danemu użytkownikowi identyfikatora oraz praw dostępu do informacji chronionych w danym systemie przetwarzania,
13. powiadamia administratora danych osobowych o konieczności utworzenia identyfikatora użytkownika w systemie oraz zmianie/nadaniu uprawnień dostępu użytkownika do systemu,
14. prowadzi ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe,
15. prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych,
16. prowadzi ewidencję miejsc przetwarzania danych osobowych w systemach informatycznych,
17. prowadzi rejestr zbiorów danych osobowych szkoły (przetwarzanych metodą tradycyjną lub w systemach informatycznych).

§20.

I.Administrator danych osobowych zobowiązany jest do przestrzegania wszystkich przepisów ustawy o ochronie danych, w szczególności poprzez:

1. określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych,
2. określenie budynków, pomieszczeń lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,

3. zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,
4. wykonywania zaleceń Inspektora Ochrony Danych w zakresie ochrony danych osobowych,
5. wdrażanie i nadzorowanie przestrzegania Polityki bezpieczeństwa informacji,
6. wdrażanie i nadzorowanie przestrzegania instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
7. działanie zgodnie z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych,
8. stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych,
9. odpowiedzialność za poprawność merytoryczną danych gromadzonych w systemach informacyjnych,
10. określanie, które osoby i na jakich prawach mają dostęp do danych informacji,

§21.

I. Administrator szkolnej sieci komputerowej odpowiedzialny jest za:

1. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
2. optymalizację wydajności systemu informatycznego, baz danych,
3. instalacje i konfiguracje sprzętu sieciowego i serwerowego,
4. instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego,
5. konfigurację i administrację oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
6. współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
7. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
8. zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
9. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,

10. przyznawanie na wniosek Administratora Danych Osobowych, za zgodą Inspektora Ochrony Danych ściśle określonych praw dostępu do informacji w danym systemie,
11. wnioskowanie do Administratora Danych Osobowych w sprawie procedur bezpieczeństwa i standardów zabezpieczeń,
12. zarządzanie licencjami, procedurami ich dotyczącymi,
13. prowadzenie profilaktyki antywirusowej.

VIII. PRZETWARZANIE DANYCH OSOBOWYCH

§22.

1. Przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach zamykanych na klucz przez wyznaczone do tego celu osoby.
2. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§23.

1.Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy niszczyć w stopniu uniemożliwiającym ich odczytanie.

2.Urządzenia, dyski lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych osobowych.

IX. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI PRZETWARZANYCH DANYCH

§24.

I. W szkole rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

1. Zabezpieczenia fizyczne:
   a. pomieszczenia zamykane na klucz,
   b. szafy pancerne z zamkami,

2. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
   a. przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
   b. przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.
3. Zabezpieczenia organizacyjne:
   a. w trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,
   b. przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszone,
   c. w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione,
   d. po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

X. ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

§25.

1. Archiwizacja informacji zawierających dane osobowe odbywa w formie elektronicznej oraz papierowej. Nośniki danych przechowywane są w wydzielonych pomieszczeniach, które są zabezpieczone przed dostępem osób nieupoważnionych.

XI. Załączniki

Załącznik nr 1: Oświadczenie o zachowaniu poufności i zapoznaniu się z przepisami,

Załącznik nr 2: Upoważnienie nr … do przetwarzania danych osobowych,

Załącznik nr 3: Odwołanie upoważnienia nr … do przetwarzania danych osobowych,

Załącznik nr 4: Ewidencja osób upoważnionych do przetwarzania danych osobowych,

Załącznik nr 5: Dostęp do kluczy i pomieszczeń, w których przetwarzane są dane,

Załącznik nr 6: Sposób przepływu danych osobowych pomiędzy poszczególnymi systemami,

Załącznik nr 7: Wykaz zbiorów danych osobowych ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów, wskazanie zawartości poszczególnych pól i powiązań między nimi,

Załącznik nr 8: Instrukcja korzystania z monitoringu wizyjnego w Zespole Szkół Chemiczno-Elektronicznych im. Jana Pawła II w Inowrocławiu,

Załącznik nr 9: Rejestr Naruszeń Danych osobowych w ZSCHE im. Jana Pawła II w Inowrocławiu,

Załącznik nr 10: Rejestr incydentów naruszenia ochrony danych osobowych,

Załącznik nr 11: Rejestr praw osób, których dane dotyczą realizowanych na żądanie.