P O L I T Y K A
B E Z P I E C Z E Ń S T W A
O C H R O N Y D A N Y C H O S O B O W Y C H

A K A D E M I C K I E G O L I C E U M
O G Ó L N O K S Z T A Ł C Ą C E G O P O L I T E C H N I K I
W R O C Ł A W S K I E J

WROCŁAW styczeń 2025

POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

Realizując postanowienia Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – jej aktualne brzmienie, ustawy o ochronie danych osobowych (jej aktualne brzmienie) oraz wydane w oparciu o delegację ustawową przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informacyjne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) z późniejszymi zmianami, postanawiam wprowadzić reguły oraz zasady pozwalające na zapewnienie ochrony danych osobowych w Akademickim Liceum Ogólnokształcącym Politechniki Wrocławskiej (dalej ALO), wybrzeże Stanisława Wyspiańskiego 23, 50-370 Wrocław

ZOBOWIĄZUJĘ

wszystkie osoby do bezwzględnego przestrzegania podanych w niniejszym opracowaniu reguł i zasad tworzących politykę bezpieczeństwa.

CZĘŚĆ OGÓLNA

1. Postanawiam objąć w ramach polityki bezpieczeństwa dane osobowe, którymi zgodnie z aktem prawnym wymienionym na wstępie są wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
2. Stosować reguły i zasady do przetwarzania danych osobowych prowadzonych zarówno w pismach, notatkach, kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych.
3. Celem polityki bezpieczeństwa jest takie postępowanie, aby osoby upoważnione do przetwarzania danych osobowych w pełni zabezpieczyły dostęp do nich przed osobami nieupoważnionymi i zabezpieczyły je oraz gromadziły w zbiorach zgodnie z wymogami obowiązującego prawa.
4. Traktować całokształt działań jako ochronę prywatności osób, których dane są przetwarzane oraz jako wymóg ustawowy.

CZĘŚĆ SZCZEGÓŁOWA

1. Obszar, w którym przetwarzane są dane osobowe stanowią budynki oraz pomieszczenia ALO, wybrzeże Stanisława Wyspiańskiego 23, 50-370 Wrocław, które posiadają następujące zabezpieczenia:
   - nieruchomość to budynek wielopoziomowy. Wejście kontrolowane jest przez pracownika ochrony obiektu całodobowo, a cały obiekt monitorowany jest przez system kontroli wizyjnej – system kamer przemysłowych,
   - wszystkie wejścia do budynków zamykane są drzwiami na zamki patentowe,
   - pomieszczenia posiadają okna z okuciami przeciwwłamaniowymi,
   - budynek posiada system alarmowy antywłamaniowy, instalację przeciwpożarową, a budynek ma zainstalowaną instalację odgromową,
   - ustalony wewnętrzny system zabezpieczenia pomieszczeń oraz zasady pobierania kluczy, ustalony sposób zabezpieczenia dokumentów w szafach wyposażonych w zamki patentowe, szyfrowe, centralne.

2. Włączam do polityki bezpieczeństwa jako jej integralną część następujące załączniki:
   - Załącznik nr 1 Instrukcja zabezpieczenia zbiorów danych osobowych przetwarzanych metodą tradycyjną
   - Załącznik nr 2 Ewidencji pracowników ALO, wybrzeże Stanisława Wyspiańskiego 23, 50-370 Wrocław pracujących poza regulaminowym czasem pracy lub w dni wolne od pracy.
   - Załącznik nr 3 Wewnętrzny system zabezpieczeń oraz zasady pobierania kluczy do pomieszczeń
   - Załącznik nr 4 Wewnętrzny system zabezpieczeń systemu komputerowego oraz użytkowania telefonów komórkowych
   - Załącznik nr 5 Oświadczenie pracownika

Załącznik nr 1
do Polityki Bezpieczeństwa
Ochrony Danych Osobowych

INSTRUKCJA ZABEZPIECZENIA ZBIORÓW DANYCH OSOBOWYCH PRZETWARZANYCH METODĄ TRADYCYJNĄ

1. Zbiory danych osobowych przetwarzanych tradycyjnie /kartoteki, skorowidze, księgi, wykazy i inne zbiory ewidencyjne/ przechowywane są w szafach zamkniętych na klucz, ewentualnie w oddzielnych pomieszczeniach specjalnie zabezpieczonych przed dostępem osób nieupoważnionych.
2. Pomieszczenia, w których znajdują się zbiory danych osobowych znajdujące się w całym budynku, posiadają okna odpowiednio zabezpieczone okuciami antywłamaniowymi.
3. Pomieszczenia, w których znajdują się zbiory danych osobowych oraz, w których przetwarzane są dane osobowe, są zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych w sposób uniemożliwiający dostęp do nich osób trzecich.
4. Przebywanie wewnątrz obszaru, w którym przetwarzane są dane osobowe osób nieupoważnionych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub za zgodą administratora danych lub osoby przez niego upoważnionej.
5. Klucze do szaf i specjalnych pomieszczeń, w których przechowywane są zbiory danych osobowych posiada pracownik upoważniony do przetwarzania danych osobowych, a w razie jego nieobecności osoba uprawniona wyznaczona przez administratora danych lub osoba przez niego upoważniona.
6. Klucze do pomieszczeń biurowych są nieoznakowane. Klucze do pomieszczeń, w których przetwarzane są dane osobowe przechowywane są przez upoważnionych do tego pracowników. Po opuszczeniu miejsca pracy pracownik deponuje klucz od pomieszczeń służbowych w bezpiecznym i niedostępnym dla innych osób miejscu.
7. Sposoby przechowywania i udostępniania kluczy określa załącznik nr 3 do Polityki Bezpieczeństwa.
8. Pracownik zatrudniony przy przetwarzaniu danych osobowych przed rozpoczęciem pracy sprawdza, czy zabezpieczenia urządzeń, w których przechowywane są zbiory danych nie zostały naruszone.
9. W przypadku stwierdzenia, że zostały naruszone zabezpieczenia urządzeń osoba ujawniająca powiadamia administratora danych lub inną upoważnioną przez niego osobę, która podejmie odpowiednie kroki w celu wyjaśnienia sprawy.
10. Za przechowywanie zbiorów danych, przetwarzanie i udostępnianie informacji ze zbioru danych osobowych odpowiada bezpośrednio pracownik upoważniony do przetwarzania danych osobowych, a w przypadku jego nieobecności osoba upoważniona przez administratora danych.
11. Po zakończeniu pracy pracownik zatrudniony przy przetwarzaniu danych zobowiązany jest zabezpieczyć należycie zbiory danych /kartoteki, skorowidze, księgi, wykazy i inne zbiory ewidencyjne/ przed dostępem osób trzecich, pomieszczenie zamknąć na klucz.
12. W przypadku utraty kluczy od pomieszczenia lub szafy, w której przechowywane są zbiory danych osobowych, należy wszcząć postępowanie wyjaśniające i dokonać wymiany zamków.
13. Administrator danych podejmuje odpowiednie przedsięwzięcia, mające na celu należyte zabezpieczenie danych osobowych w czasie remontu pomieszczeń, naprawy urządzeń i sprzętu oraz w czasie zmiany

lokalizacji jednostki organizacyjnej lub w trakcie opuszczania pomieszczeń, jak również w czasie innych okoliczności zakłócających normalny tok pracy.

14. Dokumenty zawierające dane osobowe, które utraciły swoje praktyczne lub przedmiotowe znaczenie i nie podlegają trwałemu przechowywaniu mogą być zniszczone w warunkach gwarantujących ochronę danych osobowych w sposób uniemożliwiający ich odtwarzanie.
15. Zniszczenia dokumentów zawierających dane osobowe dokonuje pracownik upoważniony do przetwarzania danych osobowych, sporządzając protokół zniszczenia potwierdzony przez Administratora Danych.

Wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe

1. Przetwarzaniem danych osobowych jest wykonywanie jakichkolwiek operacji na danych osobowych, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza tych, które wykonuje się w systemie informatycznym.
2. Dane osobowe przetwarzane są na terenie Akademickiego Liceum Ogólnokształcącego Politechniki Wrocławskiej w budynku C-13 należącym do Politechniki Wrocławskiej, pod adresem wyb. Wyspiańskiego 23-25 we Wrocławiu.
3. Ze względu na nagromadzenie danych osobowych szczególnie chronione powinny być następujące pomieszczenia:

GABINET DYREKTORA SZKOŁY – piętro II gabinet 2.34b
SEKRETARIAT – piętro II gabinet 2.34a
GABINET WICEDYREKTORA – piętro IV gabinet 4.38
POKÓJ NAUCZYCIELSKI – piętro II gabinet 2.34
BIURO KSIĘGOWEJ – piętro III gabinet 3.32
BIURO SPECJALISTY DS. KADR I PŁAC – piętro III gabinet 3.32
POKÓJ PEDAGOGA SZKOLNEGO – piętro III gabinet 3.25
ARCHIWUM – piętro III, gabinet 3.23
POKÓJ SPECJALISTY DS. ADMINISTRACJI – piętro III gabinet 3.26
POKÓJ ADMINISTRATORA DZIENNIKA LIBRUS – piętro I gabinet 1.10
POKÓJ PIELĘGNIARSKI – piętro III gabinet 3.28
BIBLIOTEKA – piętro II gabinet 2.01

§ 6 Wykaz zbiorów danych osobowych oraz struktura zasobów przetwarzanych danych w Akademickim Liceum Ogólnokształcącym Politechniki Wrocławskiej.

Nr	Nazwa zbioru/nazwa zasobu danych	Struktura zbioru	Program/ Miejsce/ Dostęp
KANDYDACI DO SZKOŁY			
1.	Listy kandydatów do szkoły (podania o przyjęcie ucznia do szkoły)	Nazwiska i imiona, imiona rodziców, data i miejsce urodzenia, adres zameldowania i zamieszkania, pesel, wizerunek, telefon.	Dział Rekrutacji PWRj/ Sekretariat ALO PWr
2.	Dokumenty rekrutacyjne kandydatów nieprzyjętych do szkoły	Nazwiska i imiona, imiona rodziców, data i miejsce urodzenia, adres zameldowania i zamieszkania, pesel, wizerunek, telefon.	Sekretariat ALO PWr
3.	Dane rekrutacyjne uczniów przyjętych; w wersji papierowej z podziałem na odziały i rok szkolny.	Nazwiska i imiona, imiona rodziców, data i miejsce urodzenia, adres zameldowania i zamieszkania, pesel, wizerunek, telefon.	Sekretariat ALO PWr
4.	Oryginały świadectw szkolnych oraz zaświadczeń sprawdzianów wiedzy szóstoklasisty oraz egzaminu gimnazjalnego.	Nazwiska i imiona, imiona rodziców, data i miejsce urodzenia, adres zameldowania i zamieszkania, pesel.	Sekretariat ALO PWr
5.	Listy uczniów przyjętych do szkoły	Nazwisko i imię ucznia, data i miejsce urodzenia, pesel, adresy zamieszkania ucznia, nazwiska i imiona rodziców, adres rodziców, Przyjęcie do szkoły: data, klasa/semestr.	Dział Rekrutacji PWR/ Sekretariat ALO PWr
UCZNIOWIE SZKOŁY			
6.	Księga uczniów – zbiór danych o uczniach	Nazwisko i imię ucznia, data i miejsce urodzenia, pesel, adresy zamieszkania ucznia, nazwiska i imiona rodziców, adres rodziców, Przyjęcie do szkoły: data, klasa/semestr.	Sekretariat ALO PWr
7.	Dzienniki lekcyjne (dziennik Librus w wersji elektronicznej oraz wydruki z systemu zawierające dane osobowe)	Nazwisko i imiona uczniów, nr ewidencyjny ucznia, data urodzenia, miejsce urodzenia, pesel, miejsce zamieszkania, Imiona i nazwiska rodziców (opiekunów), adres rodziców (opiekunów), nr telefonu domowego, ewentualnie zakładu pracy.	Sekretariat ALO PWr
8.	Arkusze ocen uczniów	Imię i nazwisko, data urodzenia, miejsce urodzenia, pesel, data przyjęcia do szkoły, nr księgi uczniów, adres zamieszkania ucznia, imiona i nazwiska rodziców i adresy ich zamieszkania, przebieg i wyniki nauki.	Sekretariat ALO PWr
9.	Dokumentacja medyczna uczniów	Imię i nazwisko, data urodzenia, miejsce zamieszkania, stan zdrowia.	Gabinet Pielęgniarski
10.	Dokumentacja związana z obowiązkiem szkolnym, obowiązkiem nauki	Imię i nazwisko, data urodzenia, miejsce urodzenia, pesel.	Sekretariat ALO PWr
11.	Dokumentacja pedagoga – dokumentacja badań i czynności uzupełniających prowadzonych przez pedagoga w tym orzeczenia i opinie Poradni Psychologiczno-Pedagogicznej	Imię i nazwisko, data urodzenia, miejsce zamieszkania, stan zdrowia.	Gabinet Pedagoga
12.	Dokumentacja związana z indywidualnym programem nauczania (umowy z nauczycielami prowadzącymi zajęcia)	Imię i nazwisko rodzica, adres zamieszkania, imię i nazwisko ucznia,	Dyrekcja szkoły
13.	Ewidencja decyzji dyrektora szkoły takich jak np.: Indywidualne nauczanie uczniów, zwolnienie z zajęć w-f, usprawiedliwienia, naganny.	Imię i nazwisko rodzica, adres zamieszkania, imię i nazwisko ucznia,	Sekretariat ALO PWr
14.	Deklaracje uczęszczania na religię, etykę; sprzeciw od zajęć z wychowania do życia w rodzinie	Imię i nazwisko rodzica, adres zamieszkania, imię i nazwisko ucznia, przynależność wyznaniowa	Wychowawcy klas

15.	Biblioteka	Imię i nazwisko ucznia, pesel, data urodzenia, miejsce urodzenia, adres, dane o wypożyczeniach.	Biblioteka Politechniki Wrocławskiej
16.	Lista uczestników wycieczek	Imię i nazwisko, pesel, adres zamieszkania, telefon	Gabinet Wicedyrektora szkoły
17.	Rejestr wydanych kluczy do szafek szkolnych uczniów	Imię i nazwisko	Sekretariat ALO PWr
18.	Legitymacje elektroniczne + rejestr wydanych legitymacji szkolnych	Imię i nazwisko, dane szkoły	Sekretariat ALO PWr
19.	Rejestr olimpiad (kwestie sporne)	Imię i nazwisko	Sekretariat ALO PWr
20.	Rejestr polisy grupowe i indywidulane uczniów	Imię i nazwisko, data urodzenia, miejsce urodzenia, pesel	Sekretariat ALO PWr
21.	Rejestr zdarzeń losowych i wypadków uczniów	Imię i nazwisko, data urodzenia, miejsce urodzenia, pesel	Sekretariat ALO PWr
22.	Rejestr oświadczeń uczniów	Imię nazwisko, nr legitymacji i klasa	Sekretariat ALO PWr
23.	Dokumenty uczniów wypisanych ze szkoły	Nazwiska i imiona, imiona rodziców, data i miejsce urodzenia, adres zameldowania i zamieszkania, pesel, wizerunek dziecka, telefon.	Sekretariat ALO PWr
24.	Pomoc Społeczna	Nazwiska i imiona, imiona rodziców, data i miejsce urodzenia, adres zameldowania i zamieszkania, pesel, telefon.	Pedagog
		PRACOWNICY	
25.	Akta osobowe pracowników szkoły	Imię i nazwisko, nazwisko rodowe, imiona rodziców, data urodzenia, miejsce urodzenia, PESEL, NIP, adres zameldowania, adres zamieszkania, obywatelstwo, numer i seria dowodu osobistego, imiona i nazwiska, data urodzenia dzieci pracownika, imię i nazwisko, adres i telefon osoby, którą należy powiadomić o wypadku pracownika, w przypadku mężczyzn dane dotyczące powszechnego obowiązku obrony, wykształcenie, dotychczasowe zatrudnienie.	Gabinet 3.32 – Kadry/Płace
26.	Dokumentacja dotycząca polityki kadrowej: opiniowanie awansów, podwyżek, premii.	Imię i nazwisko, data urodzenia, adres zamieszkania, przebieg zatrudnienia, wykształcenie	Gabinet 3.32 – Kadry/Płace
27.	Ewidencja zwolnień pracowników	Imię i nazwisko, data urodzenia, adres zamieszkania, przebieg zatrudnienia.	Gabinet 3.32 – Kadry/Płace
28.	Wykaz ekwiwalentów ze pranie i używanie odzieży własnej do celów służbowych	Imię i nazwisko, stanowisko	Gabinet 3.32 – Kadry/Płace
29.	Rejestr pełnomocnictw	Imię i nazwisko, stanowisko	Gabinet 3.32 – Kadry/Płace
30.	Protokoły Rad pedagogicznych	Imiona i nazwiska nauczycieli, imiona i nazwiska uczniów	Administracja Szkoły
31.	Umowy - zlecenia/dzieło zawierane z osobami fizycznymi oraz firmami, płatne i nieodpłatne wykonanie usługi.	Nazwa, siedziba, KRS, NIP, REGON, kapitał zakładowy, Imię, nazwisko, stanowisko osoby reprezentującej.	Gabinet 3.32 – Kadry/Płace
32.	Listy obecności pracowników	Imię i nazwisko	Sekretariat ALO
33.	Rejestr nieobecności w pracy nauczycieli	Imię i nazwisko	Gabinet 3.32 – Kadry/Płace
34.	Ewidencja urlopów pracowników (wnioski urlopowe)	Imię i nazwisko, stanowisko, wymiar urlopu, wykorzystanie urlopów.	Gabinet 3.32 – Kadry/Płace
35.	Wykaz badań okresowych pracowników	Imię i nazwisko, data urodzenia, PESEL, miejsce zamieszkania, stanowisko	Gabinet 3.32 – Kadry/Płace

36.	Zaświadczenia dotyczące zgody na publikowanie wizerunku	Imię i nazwisko ucznia/ nauczyciela	Gabinet 3.32 – Kadry/Płace
37.	Deklaracje ubezpieczeniowe pracowników i ich rodzin	Imię i nazwisko, nazwisko rodowe, imiona rodziców, data i miejsce urodzenia, PESEL, NIP, adres zameldowania i zamieszkania, obywatelstwo, numer i seria dowodu osobistego, imię i nazwisko, adres i telefon osoby upoważnionej do odbioru świadczenia w razie śmierci pracownika, wysokość składki i ewentualnie otrzymanych świadczeń.	Gabinet 3.32 – Kadry/Płace
38.	Arkusz organizacyjny szkoły	Imię i nazwisko, wykształcenie, pensum.	Gabinet Dyrektora
39.	Rejestr wypadków pracowników, ewidencja podejrzeń o chorobę zawodową		Sekretariat ALO PWr /BHP
40.	Księga druków ścisłego zarachowania	Imię i nazwisko, wydane świadectwa	Sekretariat ALO PWr
41.	Wykaz nadanych przesyłek pocztowych/ Dziennik korespondencyjny	Imię i nazwisko, adres zamieszkania.	Sekretariat ALO PWr
42.	Porozumienia		Sekretariat ALO PWr
43.	Protokoły pokontrolne		Sekretariat ALO PWr
44.	Zbiór upoważnień	Imię i nazwisko, stanowisko, zakres upoważnienia.	Sekretariat ALO PWr
45.	Rejestr delegacji służbowych	Imię i nazwisko, miejsce zamieszkania.	Sekretariat ALO PWr
46.	Dzienniki zajęć dodatkowych - archiwum		Archiwum
47.	Księga kontroli ALO PWr		
KSIĘGOWOŚĆ I FINANSE			
48.	Deklaracje i kartoteki ZUS pracowników	Imię i nazwisko, nazwisko rodowe, imiona rodziców, data urodzenia, miejsce urodzenia, PESEL, NIP, adres zameldowania i zamieszkania, obywatelstwo, imiona i nazwiska, data urodzenia dzieci pracownika, wymiar czasu pracy.	Głowna Księgowa
49.	Listy płac, kartoteki zarobkowe pracowników, kartoteki ZFŚS	Imię i nazwisko, data urodzenia, PESEL, miejsce zamieszkania, stopień awansu, składniki wynagrodzeń i potrąceń, okres zwolnienia, imię i nazwisko, specjalność i nr lekarza wystawiającego zwolnienie lekarskie,	Głowna Księgowa
50.	Deklaracje podatkowe pracowników	Imię i nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, PESEL, NIP, adres.	Głowna Księgowa
51.	Rejestr zaświadczeń wydawanych pracownikom szkoły	Imię i nazwisko, imiona rodziców, data i miejsce urodzenia, PESEL, NIP, adres zamieszkania, wysokość wynagrodzenia, okres zatrudnienia.	Głowna Księgowa
52.	Umowy o świadczenie usług	Nazwa, siedziba, KRS, NIP, REGON, kapitał zakładowy, Imię, nazwisko, stanowisko osoby reprezentującej.	Głowna Księgowa
53.	Rejestr deklaracji służbowych	Imię i nazwisko, imiona rodziców, data i miejsce urodzenia, PESEL, NIP, adres zamieszkania, wysokość wynagrodzenia, okres zatrudnienia.	Głowna Księgowa
54.	Nakazy komornicze	Imię i nazwisko, imiona rodziców, data i miejsce urodzenia, PESEL, NIP, adres zamieszkania, wysokość wynagrodzenia, okres zatrudnienia.	Głowna Księgowa
55.	Konto Bankowe – ibiznes SANTANDER	Numer konta, dane szkoły	Głowna Księgowa/ Dyrektor szkoły

56.	Przelewy i faktury	Nazwiska, imiona, adresy zamieszkani, nazwa, nr konta bankowego kontrahentów, NIP, REGON, nr telefonu.	Głowna Księgowa

Struktura informatyczna Akademickiego Liceum Ogólnokształcącego Politechniki Wrocławskiej składa się z sieci wewnętrznej, mieszczącej się w pomieszczeniach szkoły.

W szkole funkcjonuje Dziennik elektroniczny Librus. Dostęp do danych osobowych umieszczonych w dzienniku chroniony jest loginem i hasłem (odrębnym dla każdego użytkownika). Za prawo dostępu do danych dziennika elektronicznego odpowiada Administrator dziennika elektronicznego. Za ochronę bazy danych na Serwerze odpowiada firma Librus zgodnie z umową zawarta ze szkołą.

Załącznik nr 2
do Polityki Bezpieczeństwa
Ochrony Danych Osobowych

Ewidencji pracowników ALO, wybrzeże Stanisława Wyspiańskiego 23, 50-370 Wrocław pracujących poza regulaminowym czasem pracy lub w dni wolne od pracy.

L.p.	Stanowisko osoby
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

Załącznik nr 3
do Polityki Bezpieczeństwa
Ochrony Danych Osobowych

Wewnętrzny system zabezpieczeń oraz zasady pobierania kluczy do pomieszczeń ALO PWr, wybrzeże Stanisława Wyspiańskiego 23, 50-370 Wrocław

§ 1

Przechowywanie i udostępnianie kluczy

1. Klucze do pomieszczeń ALO PWr, wybrzeże Stanisława Wyspiańskiego 23, 50-370 Wrocław deponowane są na portierni, natomiast klucze do pomieszczeń przechowywane są bezpośrednio przez osoby uprawnione – pouczone o wadze dostępu do pomieszczeń, w których znajdują się dane osobowe. Ze zobowiązaniem do najwyższej troski o zachowanie bezpieczeństwa.
2. Po utracie jakiegokolwiek klucza należy zmienić zamek, do którego klucz został utracony.

§ 2

Zabezpieczenie pomieszczeń

1. Po zakończeniu pracy pracownicy zobowiązani są do zabezpieczania wszystkich dokumentów zawierających dane osobowe.
2. Pracownik po przyjściu do pracy sprawdza pomieszczenie, czy cokolwiek nie zostało naruszone. W razie naruszenia powiadamia Administratora.

Załącznik nr 4
do Polityki Bezpieczeństwa
Ochrony Danych Osobowych

Wewnętrzny system zabezpieczeń systemu komputerowego
oraz użytkowania telefonów komórkowych

System informatyczny – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
Opis zdarzeń naruszających bezpieczeństwo danych osobowych.
Zdarzenia zagrażające bezpieczeństwu danych osobowych podzielono na:

- zagrożenia zamierzone, świadome i celowe – istnieje możliwość naruszenia poufności danych, poprzez nieuprawniony dostęp z zewnątrz lub wewnątrz do systemu informatycznego, przejęcia lub podglądu tych danych przez osoby nieupoważnione,
- losowe wewnętrzne takie jak: awarie sprzętowe, błędy oprogramowania itd. Istnieje niebezpieczeństwo zniszczenia danych, naruszenia poufności danych,
- losowe zewnętrzne takie jak: klęski żywiołowe, przerwy w zasilaniu itp.; ich występowanie może prowadzić do utraty integralności danych, zniszczenia i uszkodzenia infrastruktury technicznej systemu, nie dochodzi do naruszenia poufności danych.

Główne zdarzenia naruszające bezpieczeństwo danych osobowych lub zakwalifikowane jako uzasadnione podejrzenie naruszenia to:

- nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu np.: zalanie pomieszczeń, katastrofa budowlana itp.;
- nadmierna wilgotność, wysoka temperatura i inne czynniki zewnętrzne,
- awaria sprzętu lub oprogramowania, wyraźnie wskazujące na ingerencję osób trzecich,
- komunikaty alarmowe systemu lub innego oprogramowania zaangażowanego w proces utrzymywania bezpieczeństwa zbiorów danych,
- odstępstwa od oczekiwanego działania urządzeń systemu informatycznego wskazujące na możliwe naruszenie bezpieczeństwa danych,
- naruszenie integralności systemu,
- naruszenie struktury danych lub nieuprawniona modyfikacja,
- przejęcie lub podgląd danych osobowych przez osoby nieupoważnione,
- naruszenie zabezpieczeń pomieszczeń, szaf, biurek i itp., w których przechowywane są zbiory danych w postaci nośników danych lub dokumentacji papierowej.

I. Cel i zakres polityki bezpieczeństwa

Celem wdrożenia polityki bezpieczeństwa jest ochrona systemu informatycznego, jako całości, jego poszczególnych elementów, przetwarzanych przez system zbiorów danych, obszaru, w którym przetwarzane są dane osobowe, a przede wszystkim zapewnienie technicznych i organizacyjnych uwarunkowań mających wpływ na zarządzanie systemami informatycznymi, w których przetwarzane są dane osobowe.

Polityka bezpieczeństwa zakłada pełne zaangażowanie wszystkich pracowników dla zapewnienia bezpieczeństwa danych osobowych przetwarzanych w sposób tradycyjny oraz za pomocą systemów informatycznych.
Dla skutecznej realizacji zasad i reguł polityki bezpieczeństwa zapewnione są:

- odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne,
- szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony,
- monitorowanie zastosowanych środków ochrony.

Każdy pracownik posiada do dyspozycji komputer służbowy z zindywidualizowanym dostępem.
Każdy pracownik posiadający dostęp do komputera, zobowiązany jest zabezpieczać dostęp do urządzenia i uniemożliwić innym osobom korzystanie z niego.
Komputer może być włączony jedynie w czasie obecności pracownika, w którego jest dyspozycji.
Komputer powinien być zabezpieczony hasłem.
Awarie lub utrata komputera winny być natychmiast zgłoszone Administratorowi.
Naprawa komputera może być dokonywana jedynie w obecności pracownika, w sposób uniemożliwiający korzystanie z zasobów komputera.

Służbowy telefon komórkowy może zostać przekazany pracownikowi. Każdy telefon musi zostać zabezpieczony przez jego użytkownika, przy włączeniu: kod pin, po zakończeniu rozmowy hasło cyfrowe lub graficzne.

II. Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej

1. Zabezpieczenia infrastruktury przed skutkami awarii zasilania
   Zastosowano: wydzieloną sieć elektroenergetyczną, oraz listwy przepięciowe.
2. Zabezpieczenia stanowisk komputerowych wykorzystywanych do przetwarzania danych osobowych
   - Zbiór danych osobowych przetwarzany przy użyciu komputera przenośnego, wymaga zabezpieczenia w postaci hasłowania dysku twardego. Przechowywanie komputera przenośnego po zakończeniu pracy wymaga zdeponowania go w bezpiecznym miejscu.
   - Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje.
3. Zabezpieczenia przed nieuprawnionym dostępem do danych osobowych, w tym środków zapewniających rozliczalność wykonywanych operacji
   - Lokalizacja urządzeń komputerowych (komputerów, drukarek itp.) uniemożliwia osobom niepowołanym (np. innym pracownikom lub studentom) dostęp do nich.
   - Dostęp do zbioru danych osobowych, który przetwarzany jest na komputerze stacjonarnym lub przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła.
   - Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4. Zabezpieczenia sprzętowe i programowe służące ochronie poufności danych przesyłanych drogą elektroniczną (środków ochrony transmisji),
   - Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji z użyciem VPN
   - Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
5. Zabezpieczenia sprzętowe i programowe przed szkodliwym oprogramowaniem i nieuprawnionym dostępem do przetwarzanych danych
   - Zastosowano programy antywirusowe chroniące przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity
   - Użyto system Firewall oraz IDS/IPS do ochrony dostępu do sieci.

III. Zabezpieczenia baz danych i oprogramowania przetwarzającego dane osobowe

Opis technicznych i programowych środków bezpieczeństwa zastosowanych w procedurach, aplikacjach i programach oraz innych narzędziach programowych wykorzystywanych do przetwarzania danych osobowych:

1. Dostęp do zbioru danych osobowych (do bazy danych i do programu) wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
2. Zastosowano mechanizm umożliwiający automatyczną rejestrację identyfikatora użytkownika i datę pierwszego wprowadzenia danych osobowych.
3. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
4. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
5. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
6. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika - automatyczny wygaszacz ekranu.
7. Zastosowano oprogramowanie antywirusowe na stanowiskach, na których przetwarzane są dane osobowe.

IV. Procedura korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek nielegalnych programów oraz plików pobranych z niewiadomego źródła.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem)
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”

V. Procedura korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania informacji wrażliwych wewnątrz organizacji, bądź wszelkich danych osobowych poza organizację, należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne, a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”.

VI. Procedura nadawania uprawnień do przetwarzania danych osobowych

Procedura opisuje zasady: przyznawania, modyfikacji i usuwania uprawnień użytkownika do przetwarzania zbiorów w systemie informatycznym lub w wersji papierowej. Celem procedury jest minimalizacja ryzyka nieuprawnionego dostępu do danych osobowych i utraty poufności przez osoby nieupoważnione.

VII. Zarządzane uprawnieniami użytkowników

1. Przyznanie, anulowanie upoważnienia do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze papierowym realizowane jest na podstawie Upoważnienia.
2. Przed nadaniem upoważnienia, należy sprawdzić, czy osoba upoważniona:
    1. Odbyła szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych lub została zapoznana z polityką ODO.
    2. Podpisała oświadczenie o zachowaniu poufności.
    3. Będzie przetwarzać dane osobowe w zakresie i celu określonym upoważnieniem.
3. Regularnie należy aktualizować politykę upoważnień i ich zakresu (np. z powodu zatrudnienia, urlopu, dostępu do zbiorów lub zmiany stanowiska pracy).
4. Zakres uprawnień w systemach informatycznych dla danej osoby określa Załącznik.
5. Po akceptacji upoważnienia, nadawany jest identyfikator oraz uprawnienia użytkownika w systemach informatycznych i aplikacjach.
6. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
7. Należy prowadzić ewidencję osób upoważnionych do przetwarzania danych osobowych.

VIII. Zarządzanie uprawnieniami administratorów

1. Administratorów systemów informatycznych (ASI) powołuje Administrator.
2. Hasło znane jest tylko administratorowi odpowiedzialnemu za dany system i zdeponowane jest w bezpiecznej kopercie w Sekcji IT.
3. W przypadkach awaryjnych (np. nieobecność administratora) hasło może być przekazane osobie zastępującej administratora za zgodą i wiedzą Administratora.

IX. Metody i środki uwierzytelnienia

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

X. Ogólne zasady postępowania z hasłami

1. ASI informuje mailem lub ustnie użytkownika o nadaniu pierwszego hasła do systemu.
2. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.
3. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
4. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
5. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
6. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

XI. Hasła do programów przetwarzających dane osobowe

1. Hasło dostępu do programów składają się co najmniej z 8 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Zaleca się zmianę hasła raz na 30 dni lub zmianę hasła wymusza system.

XII. Procedura rozpoczęcia, zawieszenia i zakończenia pracy

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

- Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.
- Użytkownik jest zobowiązany do powiadomienia właściciela firmy o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
- Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. pracownikom innych działów) wglądu do danych wyświetlanych na monitorach komputerowych.

- Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wylogować się z systemu.
- Po zakończeniu pracy, użytkownik zobowiązany jest:
  - wylogować się z systemu, a następnie wyłączyć sprzęt komputerowy,
  - zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki elektroniczne i tradycyjne, na których znajdują się dane osobowe.

XIII. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków

Procedura określa sposób postępowania z nośnikami: twardymi dyskami, płytami CD/DVD, pamięciami typu „flash" na których znajdują się dane osobowe, celem zabezpieczenia ich przez zniszczeniem, kradzieżą, dostępem osób nieupoważnionych.

XIV. Zabezpieczenie elektronicznych nośników informacji

1. Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych)
2. Zabrania się wynoszenia poza obszar organizacji wymiennych nośników informacji, a w szczególności twardych dysków z zapisanymi danymi osobowymi bez zgody właściciela firmy.
3. W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji należy stosować następujące zasady bezpieczeństwa:
   a. adresat powinien zostać powiadomiony o przesyłce,
   b. nadawca powinien sporządzić kopię przesyłanych danych,
   c. dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą,
   d. stosować bezpieczne koperty depozytowe,
   e. adresat powinien powiadomić nadawcę o otrzymaniu przesyłki.
4. Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji, po ustaniu powodu ich przechowywania.
5. Podlegające likwidacji uszkodzone lub przestarzałe nośniki, w szczególności twarde dyski z danymi osobowymi, są komisyjnie niszczone w sposób fizyczny (Załącznik 6).
6. Nośniki informacji zamontowane w sprzęcie IT, a w szczególności twarde dyski z danymi osobowymi, powinny być wymontowane lub wyczyszczone specjalistycznym oprogramowaniem, zanim zostaną przekazane poza obszar organizacji.

XV. Zabezpieczenie dokumentów i wydruków

1. Dokumenty i wydruki trwałe z danymi osobowymi przechowuje się w archiwum lub w zabezpieczonych fizycznie pomieszczeniach, biurkach i szafach.
2. Pracownicy są zobowiązani do zabezpieczania dokumentów (np. Zamykanie dokumentów na klucz w szafach, biurkach) przed dostępem osób nieupoważnionych podczas swojej nieobecności w pomieszczeniach lub po zakończeniu pracy (tzw. Polityka czystego biurka).
3. Zabrania się pozostawiania wydruków oraz ksero na drukarkach, skanerach i kserokopiarkach.
4. Pracownicy są zobowiązani do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.
5. Za zapewnienie bezpieczeństwa dokumentów i wydruków odpowiedzialni są kierownicy jednostek organizacyjnych oraz podległe im osoby przetwarzające dane osobowe.

XVI. Procedura zabezpieczenia systemu informatycznego, w tym przed wirusami komputerowymi

Ochrona antywirusowa

Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe.

1. System antywirusowy zainstalowano na stacjach roboczych
2. System antywirusowy zapewnia ochronę: systemu operacyjnego, przechowywanych plików, poczty elektronicznej
3. Użytkownicy zobowiązani są do skanowania plików programem antywirusowym.

4. Należy zapewnić stałą aktywność programu antywirusowego, tzn. program antywirusowy musi być aktywny podczas pracy systemu informatycznego przetwarzającego dane osobowe.
5. Aktualizacja definicji wirusów odbywa się automatycznie.
6. W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić innych pracowników oraz Dyrektora.

XVII. Aktualizacje oprogramowania

Każdy pracownik odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową, co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki) oraz odpowiada za użytkowanie licencjonowanego oprogramowania do przetwarzania danych osobowych.

……..……

(imię i nazwisko pracownika)

Załącznik nr 5
do Polityki Bezpieczeństwa
Ochrony Danych Osobowych

OŚWIADCZENIE

Oświadczam, że zapoznałem/łam się z Polityka bezpieczeństwa ochrony danych osobowych Akademickiego Liceum Ogólnokształcącego Politechniki Wrocławskiej i zobowiązuję się do jej przestrzegania oraz podejmowania wszelkich działań mających na celu realizację ochronę tych danych.

……..……
(data, czytelny podpis pracownika)