POLITYKA BEZPIECZEŃSTWA INFORMACJI

II LICEUM OGÓLNOKSZTAŁCĄCEGO W JAŚLE

JASŁO 2016

SPIS TREŚCI

Podstawa prawna

Konstytucja RP (art. 47 i 51)

Konwencja nr 108 Rady Europy – dotycząca ochrony osób w związku z automatycznym przetwarzaniem danych osobowych

Dyrektywa PE i RE z dnia 24 października 1995 r. (95/46/EC) w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych

Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2014 r. Nr 1182 ze zmianami)

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)

Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015 r. poz. 719)

Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015 r. poz. 745)

Kodeks pracy

Podstawowe pojęcia

§ 1

- Szkoła – w tym dokumencie jest rozumiana, jako II Liceum Ogólnokształcące w Jaśle, zlokalizowane przy ulicy Floriańskiej 24;
- Polityka - – w tym dokumencie jest rozumiana jako „Polityka bezpieczeństwa" obowiązująca w II Liceum Ogólnokształcącym w Jaśle;
- Instrukcja – w tym dokumencie rozumiana jest jako „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w II Liceum Ogólnokształcącym w Jaśle";
- Administrator Bezpieczeństwa Informacji (ABI) – pracownik szkoły wyznaczony przez Administratora Danych Osobowych (Dyrektora II Liceum Ogólnokształcącego w Jaśle) zgodnie z Art. 36 a Ustawy o ochronie danych osobowych;
- użytkownik systemu – osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w szkole, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w szkole;
- identyfikator użytkownika – jest to ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- Administrator Systemu Informatycznego (ASI) – pracownik odpowiedzialny za funkcjonowanie systemu teleinformatycznego, oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie;
- sieć lokalna – połączenie komputerów pracujących w szkole w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych;
- sieć publiczna – sieć telekomunikacyjna, niebędąca siecią wewnętrzną służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73 poz. 852, z poźn. zm.);
- sieć telekomunikacyjna – urządzenia telekomunikacyjne zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za pomocą przewodów, fal radiowych, bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171 poz.1800 ze zmianami);
- system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
- przetwarzanie danych – rozumie się to w tym dokumencie, jako jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;
- zabezpieczenie danych w systemie informatycznym – wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
- teletransmisja – przesyłanie informacji za pomocą sieci telekomunikacyjnej;
- aplikacja (oprogramowanie użytkowe lub oprogramowanie aplikacyjne) – każdy samodzielny program lub element pakietu oprogramowania, który nie jest zaliczany do oprogramowania systemowego lub programów usługowych (narzędziowych);
- wysoki poziom bezpieczeństwa – musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych, połączone jest z siecią publiczną,

Rozdział I
POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

I.1 Wykaz budynków w których przetwarzane są dane osobowe

§ 2

LP.	ADRES – BUDYNEK	POMIESZCZENIA
1.	38-200 Jasło, ul. Floriańska 24	gabinet dyrektora gabinet wicedyrektora sekretariat księgowość gabinet pedagoga szkolnego gabinet higienistki szkolnej biblioteka pokój nauczycielski sale lekcyjne

Kopie zapasowe zawierające zbiory danych osobowych przechowywane są w szafie stalowej w pokoju nr 34 i szafie zamykanej na klucz w pokoju 35.

I.2 Zbiory danych osobowych

§ 3

Wykaz zbiorów danych ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opisem struktury zbiorów stanowi załącznik nr 1.

§ 4

Wykaz zbiorów danych przetwarzanych w formie tradycyjnej z opisem struktury zbiorów stanowi załącznik nr 2.

I.3 System przetwarzania danych osobowych

§ 5

W skład systemu wchodzą:
- dokumentacja papierowa (dokumenty uczniów, dokumentacja przebiegu nauczania, dokumentacja kadrowo-płacowa, dokumenty księgowe, korespondencja);
- wydruki komputerowe;
- urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji;
- procedury przetwarzania danych w tym systemie, w tym procedury awaryjne.

§ 6

Sposób przepływu danych pomiędzy poszczególnymi systemami jest następujący:

KADRY ⟶ PŁATNIK

Z aplikacji **Vulcan Optimum Kadry** do programu **Prokom Płatnik** przekazywane są dane dotyczące zarejestrowania i wyrejestrowania pracowników.

Sposób przekazywania danych: manualny

PŁACE ⟶ PŁATNIK

Z aplikacji **Vulcan Optimum Płace** do programu **Prokom Płatnik** przekazywane są dane dotyczące składek na ubezpieczenia.

Sposób przekazywania danych: manualny

PŁACE ⟶ BANK SPÓŁDZIELCZY W RYMANOWIE Filia w Jaśle

Z programu **Vulcan Optimum Płace** do **Bank Spółdzielczy w Rymanowie** przekazywane są dane dotyczące należnych kwot przelewanych na konto pracowników pracowników.

Sposób przekazywania danych: manualny

NABÓR ⟶ SEKRETARIAT

Z systemu **vEdukacja Nabór** do programu **Vulcan Optimum Sekretariat** przekazywane są dane dotyczące uczniów.

Sposób przekazywania danych: manualny

Pozostałe programy są niezależne i posiadają samodzielne bazy danych. Przetwarzanie danych osobowych w systemie informatycznym odbywa się przy zachowaniu wysokiego poziom bezpieczeństwa.

I.4 Środki techniczne i organizacyjne stosowane w przetwarzaniu danych

I.4.1 Cele i zasady funkcjonowania polityki bezpieczeństwa

§ 7

Realizując Politykę bezpieczeństwa informacji zapewnia ich:
- poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom,
- integralność – dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany,
- dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot,
- rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom,

- autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
- niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,
- niezawodność – zamierzone zachowania i skutki są spójne.

§ 8

Polityka bezpieczeństwa informacji ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:
1) naruszeń danych osobowych rozumianych jako prywatne dobro powierzone Szkole;
2) naruszeń przepisów prawa oraz innych regulacji;
3) utraty lub obniżenia reputacji Szkoły;
4) strat finansowych ponoszonych w wyniku nałożonych kar;
5) zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.

§ 9

Realizując Politykę bezpieczeństwa w zakresie ochrony danych osobowych Szkoła dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
– przetwarzane zgodnie z prawem,
– zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
– merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
– przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

I.4.2 Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych

§ 10

Za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą grozi odpowiedzialność karna wynikająca z przepisów ustawy o ochronie danych osobowych lub pracownicza na zasadach określonych w kodeksie pracy.

§ 11

Administrator Danych Osobowych (ADO) – Dyrektor Szkoły:
– formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
– decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
– odpowiada za zgodne z prawem przetwarzanie danych osobowych w Szkole.

§ 12

Administrator Danych Osobowych może powołać **Administrator Bezpieczeństwa Informacji (ABI)**, który będzie realizował zadania określone w ustawie, rozporządzeniu w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych

oraz rozporządzeniu w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji.

§ 13

Administrator Systemu Informatycznego (ASI) – pracownik Szkoły wyznaczony przez ADO:
- zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa,
- doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem,
- przydziela identyfikatory użytkownikom systemu informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu,
- nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,
- zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych,
- prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

§ 14

Pracownik przetwarzający dane (PPD) – pracownik upoważniony przez ADO:
- chroni prawo do prywatności osób fizycznych powierzających Szkole swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym Szkoły,
- zapoznaje się zasadami określonymi w Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym Szkoły i składa oświadczenie o znajomości tych przepisów.

I.4.3 Zasady udzielania dostępu do danych osobowych

§ 15

Dostęp do danych osobowych może mieć wyłącznie osoba zaznajomiona z przepisami ustawy o ochronie danych osobowych oraz zasadami zawartymi w obowiązującej w Szkole Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym. Osoba zaznajomiona z zasadami ochrony danych potwierdza to w pisemnym oświadczeniu.

§ 16

Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca pisemne imienne ewidencjonowane upoważnienie wydane przez ADO. Wzór upoważnienie określa załącznik nr 3. Wzór rejestru osób upoważnionych określa załącznik nr 4.

§ 17

ADO może wyznaczyć upoważnionych do przetwarzania danych osobowych pracowników Szkoły do nadzoru nad upoważnionymi pracownikami podmiotów zewnętrznych lub innymi upoważnionymi osobami przetwarzającymi dane osobowe w Szkole.

I.4.4 Udostępnianie i powierzanie danych osobowych

§ 18

Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.

§ 19

Udostępnienie danych może nastąpić na pisemny wniosek zawierający następujące elementy:
- adresat wniosku (administrator danych),
- wnioskodawca,
- podstawa prawna (wskazanie potrzeby),
- wskazanie przeznaczenia,
- zakres informacji.

§ 20

Administrator odmawia udostępnienia danych jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

§ 21

Powierzenie danych może nastąpić wyłącznie w drodze pisemnej umowy, w której osoba przyjmująca dane zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych. Umowa powinna zawierać informacje o podstawia prawnej powierzenia danych, celu i sposobie ich przetwarzania.

§ 22

Każda osoba fizyczna, której dane przetwarzane są w Szkole, ma prawo zwrócić się z wnioskiem o udzielenie informacji związanych z przetwarzaniem tych danych, prawo do kontroli i poprawiania swoich danych osobowych, a także w przypadkach określonych w art. 32 ust 1 pkt 7 i 8 ustawy o ochronie danych osobowych prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz sprzeciwu wobec przekazywania ich innym podmiotom.

§ 23

Sprawy związane z udzielaniem informacji w tym zakresie prowadzi ADO, udzielając informacji o zawartości zbioru danych na piśmie zgodnie ze wzorem w załączniku nr 6.

I.4.5 Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej

§ 24

Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia, w których znajdują się zbiory danych osobowych musi być poprzedzone przeniesieniem zbioru danych do odpowiednio zabezpieczonego miejsca. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.

§ 25

Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych. Dostęp do pokoi jest kontrolowany za pomocą monitoringu wizyjnego.

§ 26

Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Szkole powinno odbywać się po uzyskaniu upoważnienia lub skonsultowane z ADO w przypadku osób upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

I.4.6 Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych

§ 27

Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w *Instrukcji zarządzania systemem informatycznym*, obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego szkoły. Znajomość przepisów potwierdza upoważniony pracownik poprzez złożenie oświadczenia stanowiącego załącznik nr 5.

I.5 Analiza ryzyka związanego z przetwarzaniem danych osobowych

I.5.1 Identyfikacja zagrożeń

§ 28

FORMA PRZETWARZANIA DANYCH	ZAGROŻENIA
dane przetwarzane w sposób tradycyjny	– oszustwo, kradzież, sabotaż; – zdarzenia losowe (powódź, pożar); – zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); – niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; – pokonanie zabezpieczeń fizycznych; – podsłuchy, podglądy; – ataki terrorystyczne; – brak rejestrowania udostępniania danych; – niewłaściwe miejsce i sposób przechowywania dokumentacji;

FORMA PRZETWARZANIA DANYCH	ZAGROŻENIA
dane przetwarzane w systemach informatycznych	– nie przydzielenie użytkownikom systemu informatycznego identyfikatorów; – niewłaściwa administracja systemem; – niewłaściwa konfiguracja systemu; – zniszczenie (sfałszowanie) kont użytkowników; – kradzież danych kont; – pokonanie zabezpieczeń programowych; – zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); – niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; – zdarzenia losowe (powódź, pożar); – niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania z pomocą nośników informacji i komputerów przenośnych; – naprawy i konserwacje systemu lub sieci wykonywane przez osoby nieuprawnione; – przypadkowe bądź celowe uszkodzenie lub modyfikowanie systemów i aplikacji informatycznych lub sieci; – przypadkowe bądź celowe wprowadzenie zmian do chronionych danych osobowych – brak rejestrowania zdarzeń tworzenia lub modyfikowania danych;

I.5.2 Sposób zabezpieczenia danych

§ 29

FORMA PRZETWARZANIA DANYCH	STOSOWANE ŚRODKI OCHRONY
dane przetwarzane w sposób tradycyjny	– przechowywanie danych w pomieszczeniach zamykanych na zamki patentowe; – przechowywanie danych osobowych w szafach zamykanych na klucz; – zastosowanie czujników ruchu informujących firmę ochroniarską o nieautoryzowanym wejściu do budynku; – zastosowanie monitoringu wizyjnego regulującego gospodarkę kluczami; – przetwarzanie danych wyłącznie przez osoby posiadających stosowne upoważnienie; – zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania;

FORMA PRZETWARZANIA DANYCH	STOSOWANE ŚRODKI OCHRONY
dane przetwarzane w systemach informatycznych	– kontrola dostępu do systemów; – zastosowanie programów antywirusowych i innych regularnie aktualizowanych narzędzi ochrony; – stosowanie ochrony zasilania; – systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych; – składowanie danych sensytywnych oraz nośników wymiennych i nośników kopii zapasowych w odpowiednio zabezpieczonych szafach; – zabezpieczenie pomieszczenia serwerowni; – przydzielenie pracownikom indywidualnych kont użytkowników i haseł; – stosowanie indywidualnych haseł logowania do poszczególnych programów; – właściwa budowa hasła;

I.5.3 Określenie wielkości ryzyka

§ 30

Poziom ryzyka naruszenia bezpieczeństwa danych jest niski. Zastosowane techniczne i organizacyjne środki ochrony są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

I.5.4 Identyfikacja obszarów wymagających szczególnych zabezpieczeń

§ 31

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla systemów informatycznych, stosuje się wysoki poziom bezpieczeństwa. Administrator Danych Osobowych przeprowadza okresową analizę ryzyka dla poszczególnych systemów i na tej podstawie określa środki techniczne i organizacyjne, zastosowane celem zapewnienia właściwej ochrony przetwarzanych danych.

Rozdział II
INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

II.1 Nadawanie i rejestrowanie uprawnień do przetwarzania danych w systemie informatycznym

§ 32

Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych w Szkole.

§ 33

Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada ASI.

§ 34

ASI nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia nadanego pracownikowi przez ADO.

§ 35

Usuwanie kont stosowane jest wyłącznie w uzasadnionych przypadkach, standardowo, przy ustaniu potrzeby utrzymywania konta danego użytkownika ulega ono dezaktywacji w celu zachowania historii jego aktywności.

§ 36

Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu stosunku pracy, co jest równoznaczne z cofnięciem uprawnień do przetwarzania danych osobowych.

II.2 Zabezpieczenie danych w systemie informatycznym

§ 37

Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i stacji roboczych, na których przetwarzane są dane osobowe zapewniają zasilacze UPS.

§ 38

W przypadkach awaryjnych, takich jak nagły brak zasilania, ciągłość funkcjonowania systemu informatycznego podtrzymuje bateria zasilająca serwerowni. W czasie pracy baterii zasilającej ASI dokonuje oceny sytuacji i podejmuje wszelkie niezbędne kroki w celu zachowania integralności danych oraz przywrócenia normalnego funkcjonowania systemu.

§ 39

Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień. Zmiany hasła jest wymuszona automatycznie przez system.

§ 40

Hasła do systemu stacji roboczych kontrolowanych przez kontroler domeny (PDC) mają długość przynajmniej 8 znaków (duże i małe litery oraz cyfry lub znaki specjalne) i okres ważności ustawiony na nie dłużej niż 1 miesiąc. Hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych.

§ 41

W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z ASI celem uzyskania nowego hasła.

§ 42

Hasła użytkowników uprzywilejowanych posiadających uprawnienia na poziomie administratorów systemów informatycznych objęte są takimi samymi restrykcjami dotyczącymi ich poufności jak pozostałe hasła.

§ 43

System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:

- rozpoczęcie i zakończenie pracy przez użytkownika systemu,
- operacje wykonywane na przetwarzanych danych,
- przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
- nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
- błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

§ 44

System informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:

- identyfikatora osoby, której dane dotyczą,
- osoby przesyłającej dane,
- odbiorcy danych,
- zakresu przekazanych danych osobowych,
- daty operacji,
- sposobu przekazania danych.

§ 45

Stosuje się aktywną ochronę antywirusową lub w przypadku braku takiej możliwości przynajmniej raz w tygodniu skanowanie całego systemu (w poszukiwaniu „złośliwego oprogramowania") na każdym komputerze, na którym przetwarzane są dane osobowe. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada użytkownik stacji roboczej.

II.3 Zasady bezpieczeństwa podczas pracy w systemie informatycznym

§ 46

W celu rozpoczęcia pracy w systemie informatycznym użytkownik:
1) loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła (autoryzacja użytkownika w bazie usług katalogowych),
2) loguje się do programów i systemów wymagających dodatkowego wprowadzenia unikalnego identyfikatora i hasła.

§ 47

W sytuacji tymczasowego zaprzestania pracy na skutek nieobecności przy stanowisku komputerowym należy uniemożliwić osobom postronnym korzystanie z systemu informatycznego poprzez wylogowanie się z sytemu lub uruchomienie wygaszacza ekranu chroniony hasłem.

§ 48

W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.

§ 49

Użytkownik wyrejestrowuje się z systemu informatycznego przed wyłączeniem stacji komputerowej poprzez zamknięcie programu przetwarzającego dane oraz wylogowanie się z systemu operacyjnego.

§ 50

Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo (np. w celu konserwacji sprzętu). Planowe zawieszenie prac jest poprzedzone poinformowaniem pracowników Szkoły przez ASI na co najmniej 30 minut przed planowanym zawieszeniem.

§ 51

Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia ASI w razie:
- podejrzenia naruszenia bezpieczeństwa systemu;
- braku możliwości zalogowania się użytkownika na jego konto;
- stwierdzenia fizycznej ingerencji w przetwarzana dane;
- stwierdzenia użytkowania narzędzia programowego lub sprzętowego.

§ 52

Na fakt naruszenia zabezpieczeń systemu mogą wskazywać:
- nietypowy stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem);
- wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach);
- różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych);
- inne nadzwyczajne sytuacje.

II.4 Tworzenie kopii zapasowych

§ 53

Dane systemów kopiowane są w trybie tygodniowym (kopie baz danych, kopia awaryjna systemu serwera). Kopie awaryjne danych zapisywanych w programach wykonywane są co tydzień (w ostatni dzień roboczy tygodnia po zakończeniu pracy). Kopie programów i narzędzi programowych służących do przetwarzania danych tworzy się metodą całościową każdorazowo przed aktualizacją na macierzy dyskowej.

§ 54

Odpowiedzialnym za wykonanie kopii danych i kopii awaryjnych jest pracownik obsługujący dany program przetwarzający dane. Kopie zbiorów umieszczonych na serwerze wykonywane są automatycznie dedykowanym oprogramowaniem wytworzonym we własnym zakresie.

§ 55

Dodatkowe kopie wynikające z np. zmiany platformy sprzętowej i kopie awaryjne przechowywane są w szafie metalowej w pokoju nr 34 i szafie w pokoju nr 35 Szkoły.

§ 56

Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza ASI.

§ 57

Usuwanie kopii danych następuje poprzez bezpieczne kasowanie. Nośniki danych, na których zapisywane są kopie bezpieczeństwa niszczy się trwale w sposób mechaniczny.

II.5 Udostępnienie danych

§ 58

Dane osobowe przetwarzane w systemach informatycznych mogą być udostępnione osobom i podmiotom z mocy przepisów prawa.

II.6 Przeglądy i konserwacje systemów

§ 59

Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników Szkoły lub przez upoważnionych przedstawicieli wykonawców.

§ 60

Prace wymienione w § 59 powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

§ 61

Przed rozpoczęciem prac wymienionych w § 59 przez osoby niebędące pracownikami Szkoły należy dokonać potwierdzenia tożsamości tychże osób.

II.7 Niszczenie wydruków i nośników danych

§ 62

Wszelkie wydruki z systemów informatycznych zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie ich przydatności są niszczone przy użyciu niszczarek.

§ 63

Niszczenie zapisów na nośnikach danych powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.

§ 64

Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć w niszczarce.

§ 65

Po wykorzystaniu wydruki zawierające dane osobowe powinny być niszczone w niszczarce

Rozdział III
INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH

III.1 Istota naruszenia danych osobowych

§ 66

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

- nieautoryzowany dostęp do danych,
- nieautoryzowane modyfikacje lub zniszczenie danych,
- udostępnienie danych nieautoryzowanym podmiotom,
- nielegalne ujawnienie danych,
- pozyskiwanie danych z nielegalnych źródeł.

III.2 Postępowanie w przypadku naruszenia danych osobowych

§ 67

Każdy pracownik Szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to ADO.

§ 68

Każdy pracownik Szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenie ochrony oraz ustalić przyczynę i sprawcę naruszenia ochrony.

§ 69

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ADO.

§ 70

ADO podejmuje następujące kroki:

- zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy Szkoły,
- może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
- nawiązuje kontakt ze specjalistami spoza urzędu (jeśli zachodzi taka potrzeba).

§ 71

ADO dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącego załącznik nr 7.

§ 72

ADO zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych).

III.3 Sankcje karne

§ 73

Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.

§ 74

Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych.

Załączniki

Załącznik nr 1 – Wykaz zbiorów danych ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opisem struktury zbiorów

Załącznik nr 2 – Wykaz zbiorów danych przetwarzanych w formie tradycyjnej z opisem struktury zbiorów

Załącznik nr 3 – Upoważnienie do przetwarzania danych osobowych

Załącznik nr 4 – Rejestr osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 5 – Oświadczenie pracownika o zapoznaniu się z zasadami zachowania bezpieczeństwa danych osobowych

Załącznik nr 6 – Informacja o zawartości zbioru danych

Załącznik nr 7 – Raportu z naruszenia bezpieczeństwa danych osobowych

Załącznik Nr 1
do „Polityki bezpieczeństwa
II Liceum Ogólnokształcącego w Jaśle”

WYKAZ ZBIORÓW DANYCH ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH ORAZ OPISEM STRUKTURY ZBIORÓW

ZBIÓR DANYCH OSOBOWYCH	PROGRAM INFORMATYCZNY SŁUŻĄCY DO PRZETWARZANIA ZBIORU DANYCH	STRUKTURA DANYCH
Pracownicy	Kadry	PESEL/ NIP/ imię (imiona) i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ płeć/adres stały/ numer telefonu/ e-mail/ dowód osobisty (seria i nr, wydany przez, data wydania)/ imię ojca/ imię matki/ stan cywilny i rodzinny/ numer legitymacji służbowej/ posiada gospodarstwo rolne/ emeryt/ rencista/ obywatelstwo obce/ dane osoby kontaktowej/ wykształcenie/ nazwa szkoły i rok ukończenia/ staż pracy/ historia pracy/ warunki zatrudnienia/ wysokość wynagrodzenia/ukończone kursy/ kary i nagrody/ nieobecności w pracy/ informacja o karalności/ informacje o stanie zdrowia
	Płatnik	PESEL/ NIP/ imię/nazwisko/ adres/ data i miejsce urodzenia
	Płace	PESEL/ imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ płeć/adres stały/ numer telefonu/ e-mail/ dowód osobisty (seria i nr, wydany przez, data wydania)/ imię ojca/ imię matki/ stan cywilny i rodzinny/ numer legitymacji służbowej/ posiada gospodarstwo rolne/ emeryt/ rencista/ obywatelstwo obce/ osoba kontaktowa/ wykształcenie/ nazwa szkoły i rok ukończenia/ warunki zatrudnienia/ staż pracy/ staż pracy/ tytuł zawodowy/ nieobecności w pracy
	Księgowość	PESEL/ NIP/ imię/nazwisko/ adres/ data i miejsce urodzenia/ numer konta bankowego

ZBIÓR DANYCH OSOBOWYCH	PROGRAM INFORMATYCZNY SŁUŻĄCY DO PRZETWARZANIA ZBIORU DANYCH	STRUKTURA DANYCH
Pracownicy	Inwentarz	PESEL/ NIP/ imię/nazwisko/ adres/ data i miejsce urodzenia/ numer konta bankowego
	Kasa	PESEL/ NIP/ imię/nazwisko/ adres/ data i miejsce urodzenia/ numer konta bankowego
	Magazyn	PESEL/ NIP/ imię/nazwisko/ adres/ data i miejsce urodzenia/ numer konta bankowego
	SIO	PESEL/płeć/wykształcenie/ nazwa szkoły i rok ukończenia/ warunki zatrudnienia/ staż pracy/ historia pracy, kary, nagrody/ tytuł zawodowy/ zawód wyuczony i wykonywany/ uzyskane kwalifikacje/ nieobecności w pracy

ZBIÓR DANYCH OSOBOWYCH	PROGRAM INFORMATYCZNY SŁUŻĄCY DO PRZETWARZANIA ZBIORU DANYCH	STRUKTURA DANYCH
Uczniowie	Sekretariat	PESEL/imię i nazwisko/ data i miejsce urodzenia/ płeć/adres stały /numer telefonu/e-mail/ dowód osobisty (seria, numer i rodzaj, wydany przez, data wydania)/ imiona, nazwiska i adresy rodziców (opiekunów prawnych)/ stan cywilny/ numer legitymacji szkolnej/
	eDziannik	PESEL/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ płeć/adres stały (miejscowość, ulica, numer domu, numer mieszkania)/ numer telefonu/ dowód osobisty (seria, nr i rodzaj, wydany przez, data wydania)/ imię i nazwiska rodziców (opiekunów prawnych), adresy i numer telefonu rodziców (opiekunów prawnych)/ stan cywilny/ obywatelstwo/ nieobecności w szkole/
	Świadectwa	PESEL/imię i nazwisko/ data i miejsce urodzenia/ informacje o wynikach w nauce
	OBIEG	PESEL/ imię (imiona) i nazwisko/ imiona rodziców/ adres/ data i miejsce urodzenia
	MMEDICA	PESEL/ imię i nazwisko/ adres

ZBIÓR DANYCH OSOBOWYCH	PROGRAM INFORMATYCZNY SŁUŻĄCY DO PRZETWARZANIA ZBIORU DANYCH	STRUKTURA DANYCH
Kandydaci nieprzyjęci do szkoły	vEdukacja Nabór	PESEL/imię i nazwisko/ data i miejsce urodzenia/ płeć/adres stały /numer telefonu/e-mail/ imiona, nazwiska i adresy rodziców (opiekunów prawnych)/ stan cywilny

Załącznik Nr 2
do „Polityki bezpieczeństwa
II Liceum Ogólnokształcącego w Jaśle”

WYKAZ ZBIORÓW DANYCH PRZETWARZANYCH W FORMIE TRADYCYJNEJ Z OPISEM STRUKTURY ZBIORÓW

ZBIÓR DANYCH OSOBOWYCH	DOKUMENTACJA SŁUZĄCA DO PRZETWARZANIA ZBIORU DANYCH	STRUKTURA DANYCH
Pracownicy	Akta osobowe	PESEL/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/płeć/adres stały/ numer telefonu/ e-mail/ dowód osobisty (seria i nr, wydany przez, data wydania)/ imię ojca/ imię matki/ stan cywilny i rodzinny/stosunek do służby wojskowej (dokument wojskowy, seria i numer, stopień wojskowy)/ numer legitymacji służbowej/ posiada gospodarstwo rolne/ emeryt/ rencista/ obywatelstwo obce/ osoba kontaktowa/ wykształcenie/ nazwa szkoły i rok ukończenia/ warunki zatrudnienia/ staż pracy/ historia pracy, kary, nagrody/ tytuł zawodowy/ zawód wyuczony i wykonywany/ uzyskane kwalifikacje/ nieobecności w pracy
	Ewidencja akt osobowych	imię i nazwisko/ data i miejsce urodzenia/ adres stały
	Orzeczenia lekarskie do celów sanitarno-epidemiologicznych	PESEL/ imię i nazwisko/ adres stały/ informacje o stanie zdrowia
	Oświadczenia i wnioski do funduszu socjalnego	imię i nazwisko/ adres stały/ wysokość zarobków
	Listy płac	PESEL/ imię i nazwisko/ stanowisko/ numer konta bankowego
	Karty zasiłkowe	PESEL/NIP/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały/okresy niezdolności do pracy
	Karty zarobkowe	PESEL/NIP/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały/wysokość zarobków/ warunki pracy (wymiar etatu, okres umowy)
	Informacje o zarobkach (PIT-y)	PESEL/NIP/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały/wysokość zarobków
	Zaświadczenia	PESEL/NIP/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały/wysokość zarobków/ warunki pracy

ZBIÓR DANYCH OSOBOWYCH	DOKUMENTACJA SŁUZĄCA DO PRZETWARZANIA ZBIORU DANYCH	STRUKTURA DANYCH
Pracownicy	Dokumentacja ubezpieczeniowa	PESEL/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały/ informacje o stanie zdrowia
	Protokoły powypadkowe	imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały/ informacje o stanie zdrowia
	Arkusz organizacyjny	PESEL/imię i nazwisko/ staż pracy/ historia pracy (kary, nagrody)/ tytuł zawodowy/ ukończone kursy/ uzyskane kwalifikacje/ zawód wyuczony i zawód wykonywany/ warunki zatrudnienia/ nieobecności w pracy
	Dokumentacja awansów zawodowych nauczycieli	imię i nazwisko/ data i miejsce urodzenia/ adres stały/ wykształcenie/ historia pracy/ uzyskane kwalifikacje

ZBIÓR DANYCH OSOBOWYCH	DOKUMENTACJA SŁUZĄCA DO PRZETWARZANIA ZBIORU DANYCH	STRUKTURA DANYCH
Uczniowie	Dokumentacja uczniów	PESEL/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ płeć/adres stały /numer telefonu/e-mail/ dowód osobisty (seria, nr i rodzaj, wydany przez, data wydania)/ imię i nazwiska rodziców (opiekunów prawnych), adresy rodziców (opiekunów prawnych)/stan cywilny/ numer legitymacji szkolnej/ obywatelstwo obce/osoba kontaktowa/ wykształcenie/ historia nauki/ nazwa szkoły i rok ukończenia/ numer konta/ wyznanie/ informacje o stanie zdrowia
	Księga uczniów	PESEL/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ płeć/adres stały imię, nazwiska i adresy rodziców (opiekunów prawnych)
	Księga wydanych legitymacji i legitymacje	imię i nazwisko/data urodzenia/ adres/ klasa/numer legitymacji
	Rejestr zaświadczeń i zaświadczenia	imię i nazwisko/data i miejsce urodzenia/ adres/klasa/
	Arkusze ocen	PESEL/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ płeć/adres stały (miejscowość, ulica, numer domu, numer mieszkania)/ imię, nazwiska i adresy rodziców (opiekunów prawnych)/ wyznanie

ZBIÓR DANYCH OSOBOWYCH	DOKUMENTACJA SŁUZĄCA DO PRZETWARZANIA ZBIORU DANYCH	STRUKTURA DANYCH
Uczniowie	Dzienniki lekcyjne	PESEL/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ płeć/adres stały (miejscowość, ulica, numer domu, numer mieszkania)/numer telefonu/ dowód osobisty (seria, nr i rodzaj, wydany przez, data wydania)/ imię i nazwiska rodziców (opiekunów prawnych), adresy i numer telefonu rodziców (opiekunów prawnych)/ stan cywilny/ obywatelstwo obce/ nieobecności w szkole/
	Księga absolwentów	imię i nazwisko/ numer w księdze uczniów/ numer świadectwa/ data ukończenia szkoły
	Świadectwa i duplikaty	PESEL/imię i nazwisko/ data i miejsce urodzenia/ data wydania/ uzyskane oceny
	Dokumentacja ubezpieczeniowa	PESEL/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały
	Protokoły powypadkowe	imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/ adres stały/ informacje o stanie zdrowia
	Karta zdrowia ucznia	PESEL/imię i nazwisko/ data i miejsce urodzenia/ adres/ imiona rodziców/ informacje o stanie zdrowia
	Karty szczepień	PESEL/imię i nazwisko/ data i miejsce urodzenia/ adres/ imiona rodziców/ informacje o stanie zdrowia
	Karty biblioteczne	imię i nazwisko/ data i miejsce urodzenia/ adres

ZBIÓR DANYCH OSOBOWYCH	PROGRAM INFORMATYCZNY SŁUŻĄCY DO PRZETWARZANIA ZBIORU DANYCH	STRUKTURA DANYCH
Kandydaci nieprzyjęci do szkoły	Podania o przyjęcie do szkoły z załącznikami	PESEL/imię i nazwisko/ data i miejsce urodzenia/ płeć/adres stały /numer telefonu/e-mail/ imiona, nazwiska i adresy rodziców (opiekunów prawnych)/ stan cywilny

Załącznik Nr 3
do „Polityki bezpieczeństwa
II Liceum Ogólnokształcącego w Jaśle”

Jasło, dnia ……..... r.

.....
(pieczęć Szkoły)

UPOWAŻNIENIE nr ...../20XX
do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. Nr 1182 ze zmianami)upoważniam Panią/Pana .... zatrudnioną (ego) w II Liceum Ogólnokształcącym w Jaśle na stanowisku .....do przetwarzania danych osobowych zgromadzonych w formie tradycyjnej oraz w systemach informatycznych w okresie od dnia ..... 20…. r. do ……
w zakresie określonym obowiązkach służbowych.

Wyżej wymieniona osoba została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w Szkole.

.....
(podpis Administratora Danych)

Załącznik Nr 3
do „Polityki bezpieczeństwa
II Liceum Ogólnokształcącego w Jaśle”

Jasło, dnia ……..... r.

…….
(pieczęć Szkoły)

REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Identyfikator użytkownika*	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień i podpis ADO	Data odebrania uprawnień i podpis ADO	Uwagi

* Wypełnia się tylko dla osób upoważnionych do przetwarzania danych osobowych, które zostały dopuszczone do przetwarzania danych osobowych w systemie

Załącznik Nr 5
do „Polityki bezpieczeństwa
II Liceum Ogólnokształcącego w Jaśle”

..... Jasło, dnia ……..... r.
(imię i nazwisko)

.....
(stanowisko)

OŚWIADCZENIE
o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany/a oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających ze stosunku pracy, zarówno w czasie trwania umowy , jak i po jej ustaniu.

Oświadczam, że zostałem/am poinformowany/a o obowiązujących w Szkole zasadach dotyczących przetwarzania danych osobowych, określonych w Polityce bezpieczeństwa informacji, Instrukcji zarządzania Systemem Informatycznym oraz Instrukcji postępowania w sytuacji naruszenia danych II Liceum Ogólnokształcącego w Jaśle i zobowiązuję się ich przestrzegać. W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał/a danych osobowych ze zbiorów znajdujących się w Szkole.

Zostałem/am zapoznany/a z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2014 r. Nr 1182 ze zmianami) oraz Rozporządzenia MSWiA 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). Poinformowano mnie również o grożącej, stosownie do przepisów rozdziału 8 Ustawy o ochronie danych osobowych odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, ze złamanie zasad ochrony danych osobowych, obowiązujących w II Liceum Ogólnokształcącym w Jaśle może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

.....
(podpis pracownika)

Załącznik Nr 6
do „Polityki bezpieczeństwa
II Liceum Ogólnokształcącego w Jaśle”

Jasło, dnia ……..... r.

.....
(pieczęć Szkoły)

.....
(imię i nazwisko)

.....

.....
(adres)

INFORMACJA
o zawartości zbioru danych osobowych

W związku z Pani/Pana wnioskiem z dnia …… r. o udzielenie informacji związanych z przetwarzaniem danych osobowych w II Liceum Ogólnokształcącego w Jaśle działając na podstawie art. 33 ust. 1 Ustawy o ochronie danych osobowych informuję, że zbiór danych zawiera następujące Pani/Pana dane osobowe: ……..
……...

Powyższe dane przetwarzane są w II Liceum Ogólnokształcącym w Jaśle w celu …… z zachowaniem wymaganych zabezpieczeń i zostały uzyskane ……..…….…. (podać sposób).

Powyższe dane nie były / były udostępniane …….. (podać komu) w celu …… (podać cel przekazania danych).

Zgodnie z rozdziałem 4 Ustawy o ochronie danych osobowych przysługuje Pani/Panu prawo do kontroli danych osobowych, prawo ich poprawiania, a także w przypadkach określonych w art. 32 ust. 1 pkt 7 i 8 Ustawy, prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz prawo sprzeciwu wobec przetwarzania danych w celach marketingowych lub wobec przekazywania danych innemu administratorowi danych osobowych.

.....
(podpis Administratora Danych)

Załącznik Nr 7
do „Polityki bezpieczeństwa
II Liceum Ogólnokształcącego w Jaśle”

Jasło, dnia ……..... r.

.....
(pieczęć Szkoły)

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH w II Liceum Ogólnokształcącym w Jaśle

1. Data: ..... r. Godzina: .....
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:

   .....

   .....

   .....

.....
(podpis Administratora Danyc