Załącznik nr 1
do Zarządzenia nr 14/2018. Dyrektora
II Liceum Ogólnokształcącego
w Jaśle z dnia 12 grudnia 2018 r.
w sprawie wprowadzenia Polityki Ochrony Danych
w II Liceum Ogólnokształcącym w Jaśle

POLITYKA OCHRONY DANYCH

JASŁO 2018

SPIS TREŚCI

Podstawa prawna

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1)

Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z 2018 r. poz. 1000 ze zmianami)

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247)

Podstawowe pojęcia, skróty i definicje

Na użytek niniejszego dokumentu:

1) **administrator danych osobowych** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; w niniejszym dokumencie oznacza II Liceum Ogólnokształcące im. ppłk. J. Modrzejewskiego w Jaśle reprezentowany przez dyrektora;

2) **dane osobowe** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą");

3) **możliwa do zidentyfikowania osoba fizyczna** oznacza osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

4) **dane wrażliwe** oznaczają dane szczególnej kategorii, dotyczą one pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub światopoglądowych, przynależności do związków zawodowych, stanu zdrowia, seksualności lub orientacji seksualnej, obejmują też dane genetyczne i biometryczne;

5) **zbiór danych** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

6) **przetwarzanie danych** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

7) **zgoda** osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

8) **podatności** oznacza słabość zasobu lub zabezpieczenia, która może zostać wykorzystana przez zagrożenie;

9) **zagrożenie** oznacza potencjalną przyczynę niepożądanego zdarzenia, które może powodować szkodę w przetwarzanych zbiorach danych;

10) **zabezpieczenie** oznacza środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko wystąpienia niepożądanych zdarzeń;

11) **pseudonimizacja** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,

12) **incydent** oznacza naruszenie bezpieczeństwa danych osobowych, czyli zdarzenie prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

13) **państwo trzecie** oznacza państwo nienależące do Europejskiego Obszaru Gospodarczego;

14) **ustawa** oznacza ustawę o ochronie danych osobowych z dnia 10 maja 2018 r.;

15) **RODO** oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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);

16) **KRI** oznacza Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;

17) **UODO** oznacza Urząd Ochrony Danych Osobowych, który jest organem nadzorczym w kwestiach związanych z ochroną danych osobowych.

Rozdział I
ZAŁOŻENIA POLITYKI OCHRONY DANYCH

I.1 Przedmiot regulacji

Polityka Ochrony Danych II Liceum Ogólnokształcącego im. ppłk J. Modrzejewskiego w Jaśle określa:
1) normy i zasady dotyczące przetwarzania danych osobowych,
2) obowiązki osób uczestniczących w procesach przetwarzania danych,
3) podstawowe środki techniczne i organizacyjne służące zabezpieczeniu przetwarzanych danych,
4) częstotliwość i metodologię przeprowadzania analizy ryzyka,
5) procedury postępowania w przypadku wystąpienia naruszeń.

I.2 Cele wdrożenia polityki

Wdrożenie niniejszej Polityki Ochrony Danych ma na celu:

1) utrzymanie bezpieczeństwa przetwarzanych danych osobowych, czyli zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie,
2) realizację obowiązku nałożonego na Administratora Danych Osobowych (Art. 24 ust. 2 RODO),
3) zwiększenie świadomości osób zaangażowanych w procesy przetwarzania danych osobowych,
4) zredukowanie prawdopodobieństwa wystąpienia negatywnych konsekwencji naruszeń tj.:
   - naruszeń danych osobowych rozumianych jako prywatne dobro powierzone II Liceum Ogólnokształcącemu im. ppłk J. Modrzejewskiego w Jaśle;
   - naruszeń przepisów prawa oraz innych regulacji,
   - strat finansowych ponoszonych w wyniku nałożonych kar;
   - strat finansowych ponoszonych w wyniku wypłaty odszkodowań osobom pokrzywdzonym,
   - zakłóceń w funkcjonowaniu II Liceum Ogólnokształcącego im. ppłk J. Modrzejewskiego w Jaśle spowodowanych nieprawidłowym działaniem systemów
   - utraty lub obniżenia reputacji II Liceum Ogólnokształcącego im. ppłk J. Modrzejewskiego w Jaśle.

I.3 Zakres obowiązywania

1. Polityka Ochrony Danych ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez II Liceum Ogólnokształcącego im. ppłk J. Modrzejewskiego w Jaśle .
2. Polityka ma zastosowanie do wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie
3. Polityka ma zastosowanie do wszystkich lokalizacji - pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie

4. Do stosowania zasad określonych w Polityce Ochrony Danych zobowiązani są wszyscy pracownicy, zleceniobiorcy, stażyści, praktykanci oraz inne osoby, mające dostęp do informacji podlegających ochronie.

Rozdział II
SYSTEM PRZETWARZANIA DANYCH OSOBOWYCH

II.1 Uczestnicy procesu przetwarzania danych i ich zadania

1. **Administrator Danych Osobowych (ADO)** czyli Dyrektor II Liceum Ogólnokształcącego im. ppłk J. Modrzejewskiego w Jaśle :
   1) decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
   2) odpowiada za zgodne z prawem przetwarzanie danych osobowych w II Liceum Ogólnokształcącym im. ppłk J. Modrzejewskiego w Jaśle,
   3) 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,
   4) nadaje uprawnienia do dostępu do danych (zgodnie z podrozdziałem IV.1 i IV.5).

2. **Osoba przetwarzająca dane** czyli pracownik, zleceniobiorca, stażysta lub osoba upoważniona przez Administratora do przetwarzania danych osobowych:
   1) chroni prawo do prywatności osób, których dane przetwarza,
   2) zna normy prawne dotyczące ochrony danych osobowych oraz zasady określone w Polityce danych osobowych II Liceum Ogólnokształcącego im. ppłk J. Modrzejewskiego w Jaśle i wykonuje powierzone jej zadania z uwzględnieniem tych przepisów,
   3) niezwłocznie informuje Administratora Danych lub Inspektora Ochrony Danych o wszelkich nieprawidłowościach dotyczących przetwarzania danych osobowych,
   4) stosuje środki techniczne i organizacyjne służące zabezpieczeniu danych, które przetwarza w związku z realizacją obowiązków służbowych.

3. **Inspektor Ochrony Danych** czyli osoba wyznaczona przez Dyrektora II Liceum Ogólnokształcącego im. ppłk J. Modrzejewskiego w Jaśle która jest włączana we wszystkie sprawy dotyczące ochrony danych osobowych,
   1) informuje administratora oraz pracowników przetwarzających dane osobowe o obowiązkach spoczywających na nim na mocy obowiązujących przepisów o ochronie danych i doradza mu w tej sprawie,
   2) monitoruje przestrzeganie przepisów o ochronie danych osobowych oraz regulacji wewnętrznych w tym zakresie - prowadzi działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
   3) udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitoruje ich wykonanie,
   4) współpracuje z organem nadzorczym,
   5) pełni funkcje punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem,
   6) prowadzenie rejestru czynności przetwarzania lub rejestru kategorii czynności przetwarzania.

4. **Administratora Systemu Informatycznego (ASI)**, który może być wyznaczony przez Administratora Danych:

1) zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami,
2) doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem,
3) przydziela identyfikatory użytkownikom systemu informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu,
4) nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,
5) zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych,
6) prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

W przypadku nie wyznaczenia ASI powyższe zadania realizuje Administrator Danych, lub w określonym zakresie osoba, której Administrator Danych przydzielił uprawnienia administratora danego systemu.

5. **Podmiot przetwarzający** czyli osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który na podstawie umowy powierzenia, przetwarza dane osobowe w imieniu administratora.

6. **Odbiorca** czyli osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe.

7. **Strona trzecia** czyli osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

II.2 Przesłanki legalności przetwarzania danych osobowych

1. W II Liceum Ogólnokształcącym im. ppłk J. Modrzejewskiego w Jaśle przetwarza się dane osobowe zwykłe oraz wrażliwe.
2. Dane osobowe przetwarzane są wyłącznie w następujących przypadkach:
   1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
   4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
   5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
   6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

3. Dane wrażliwe mogą być przetwarzane wyłącznie w sytuacjach określonych w art. 9 RODO i podlegają one szczególnej ochronie.
4. Przetwarzanie danych na podstawie zgody wymaga aby:
   1) zgoda na przetwarzanie danych osobowych była jednoznaczna - wyrażona w formie pisemnej lub inny sposób, umożliwiający wykazanie posiadania zgody;
   2) jeżeli zgoda wyrażana jest w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę było przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem;
   3) zgoda mogła być w dowolnym momencie wycofana i było to równie łatwe jak jej wyrażenie.
   4) wycofanie zgody nie wpływało na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem;
   5) osoba, której dane dotyczą, była poinformowana o warunkach wyrażenia zgody przed jej wyrażeniem;
   6) wycofanie zgody było równie łatwe jak jej wyrażenie;
   7) wykonanie umowy nie było uzależnione od wyrażenia zgody na przetwarzanie danych, w tym świadczenie usługi, jeśli nie jest niezbędne do wykonania tej umowy.

II.3 Zasady dotyczące przetwarzania danych osobowych

1. Dane mogą być przetwarzane wyłącznie w taki sposób, aby zapewnione były:
   1) zgodność z prawem, rzetelność i przejrzystość, czyli przetwarzanie danych zgodnie z obowiązującymi przepisami oraz w sposób czytelny i zrozumiały dla osoby, której dane dotyczą;
   2) ograniczenie celu, czyli zbieranie danych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (przetwarzanie do celów archiwalnych, naukowych, historycznych lub statystycznych jest uznawane za zgodne z pierwotnymi celami, przy czym powinno odbywać się na podstawie odrębnych przepisów);
   3) minimalizacja danych, czyli określenie zakresu przetwarzanych danych w sposób adekwatny dla celu, do realizacji którego zostały zebrane;
   4) prawidłowość, czyli dbanie o merytoryczną wartość przetwarzanych informacji (dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania należy niezwłocznie usunąć lub sprostować);
   5) ograniczenie przechowywania, czyli przechowywanie danych w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne dla realizacji celów, do których dane te zostały zebrane (dane osobowe można przechowywać przez okres dłuższy, wyłącznie w celach określonych przepisami, przy zastosowaniu odpowiednich środków technicznych i organizacyjnych);
   6) integralność i poufność, czyli przetwarzanie danych w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym, niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.
2. W przypadku zbierania danych od osoby, której one dotyczą należy poinformować ją o:
   - tożsamości i danych kontaktowych Administratora,
   - danych kontaktowych inspektora ochrony danych,
   - celu oraz podstawie prawnej przetwarzania,

- odbiorcach danych lub kategoriach odbiorców – jeżeli istnieją,
- zamiarze przekazywania danych do państw trzecich (w razie przekazywania danych - informacje o stopniu ochrony, zabezpieczeniach, możliwościach uzyskania kopii danych lub miejscu udostępnienia),
- okresie przechowywania lub kryteriach ustalania tego okresu,
- prawach przysługujących osobie, której dane są przetwarzane,
- możliwości wniesienia skargi do organu nadzorczego,
- dobrowolności lub obowiązku podania danych i ewentualnych konsekwencjach ich niepodania,
- zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu.

II.4 Prawa osób, których dane są przetwarzane

1. Osobie, której dane są przetwarzane przysługują następujące uprawnienia:
   - prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;
   - prawo do żądania sprostowania (poprawiania) danych osobowych, w przypadku stwierdzenia, że dane są nieprawidłowe lub niekompletne;
   - prawo do bycia zapomnianym tj. prawo do żądania usunięcia danych osobowych, w przypadku gdy:
     - dane nie są już niezbędne do celów, dla których były zebrane lub w inny sposób przetwarzane,
     - wniesiono sprzeciw wobec przetwarzania danych osobowych,
     - wycofano zgodę na przetwarzanie danych osobowych, na podstawie której przetwarzano dane i nie ma innej podstawy prawnej ich przetwarzania,
     - dane osobowe przetwarzane są niezgodnie z prawem,
     - dane osobowe muszą być usunięte w celu wywiązania się z obowiązku wynikającego z przepisów prawa;
   - prawo do żądania ograniczenia przetwarzania danych osobowych, w przypadku, gdy:
     - kwestionuje się prawidłowość danych osobowych,
     - przetwarzanie danych jest niezgodne z prawem, a osoba, której dotyczą sprzeciwia się ich usunięciu, żądając w zamian ograniczenia przetwarzania,
     - II Liceum Ogólnokształcące im. ppłk J. Modrzejewskiego w Jaśle nie potrzebuje już danych dla swoich celów, ale osoba, której dotyczą potrzebujesz ich do ustalenia, obrony lub dochodzenia roszczeń,
     - wniesiono sprzeciw wobec przetwarzania danych, do czasu ustalenia czy prawnie uzasadnione podstawy po stronie II Liceum Ogólnokształcącego im. ppłk J. Modrzejewskiego w Jaśle są nadrzędne wobec podstawy sprzeciwu;
   - prawo do przenoszenia danych, w przypadku gdy łącznie spełnione są następujące przesłanki:
     - przetwarzanie danych odbywa się na podstawie zawartej umowy lub na podstawie zgody,
     - przetwarzanie odbywa się w sposób zautomatyzowany;
   - prawo sprzeciwu wobec przetwarzania danych, w przypadku gdy:
     - zaistnieją przyczyny związane szczególną sytuacją osoby, której dane dotyczą, w przypadku przetwarzania danych na podstawie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej przez szkołę,
     - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez szkołę lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy, prawa i wolności osoby, której dane dotyczą(w szczególności jeżeli jest ona dzieckiem).

2. W przypadku stwierdzenia, że dane przetwarzane są niezgodnie z prawem osobie, której, przysługuje prawo wniesienia skargi do organu nadzorczego właściwego w sprawach ochrony danych osobowych tj. Urzędu Ochrony Danych.

Rozdział III
BEZPIECZEŃSTWO DANYCH OSOBOWYCH

III.1 Istota bezpieczeństwa danych osobowych

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych polega na zapewnieniu ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie.
2. Ochrona danych osobowych realizowana jest poprzez stosowanie środków organizacyjnych, środków ochrony fizycznej oraz środków technicznych, których celem jest zabezpieczenie zarówno zbiorów przetwarzanych w formie tradycyjnej jak i systemu informatycznego.

III.2 Podstawowe zasady ochrony danych

1. Stosowane zabezpieczenia poddawane są okresowej inwentaryzacji i modyfikowane adekwatnie do pojawiających się zagrożeń.
2. Czynności przetwarzania danych są ewidencjonowane w rejestrze czynności przetwarzania (na podstawie art. 30 ust. 1 RODO), który zawiera następujące elementy:
   - nazwa czynności przetwarzania
   - cel przetwarzania,
   - kategorie osób,
   - kategorie danych,
   - podstawa przetwarzania danych,
   - źródło danych,
   - planowany termin usunięcia kategorii danych,
   - nazwa współadministratora i dane kontaktowe,
   - kategorie odbiorców,
   - nazwa systemu lub oprogramowania,
   - ogólny opis techniczny i organizacyjny środków bezpieczeństwa,
   - transfer do kraju trzeciego lub organizacji międzynarodowej (w przypadku transferu nazwa kraju i podmiotu oraz dokumentacja odpowiednich zabezpieczeń),
   - osoba odpowiedzialna za zawartość rejestru.
3. W razie przetwarzania danych w imieniu innego Administratora danych (na podstawie umowy powierzenia, która powinna zawierać elementy określone w artykule 28 RODO) rejestrowane są kategorie czynności przetwarzania (na podstawie art. 30 ust. 2 RODO), który zawiera następujące elementy:
   - kategorie przetworzeń,
   - administrator,
   - ogólny opis techniczny i organizacyjny środków bezpieczeństwa,
   - czas trwania przetwarzania,
   - transfer do kraju trzeciego lub organizacji międzynarodowej (w przypadku transferu nazwa kraju i podmiotu oraz dokumentacja odpowiednich zabezpieczeń),

- osoba odpowiedzialna za zawartość rejestru.

4. Rejestr czynności przetwarzania oraz rejestr kategorii czynności przetwarzania prowadzi Inspektor Ochrony Danych.
5. Za treść wpisów zamieszczonych w rejestrach odpowiedzialność ponoszą pracownicy, którzy daną czynność realizują.
6. Kontrolę nad zawartością rejestrów sprawuje dyrektor II Liceum Ogólnokształcącego im. ppłk J. Modrzejewskiego w Jaśle, który zatwierdza wszystkie wpisy do rejestrów.
7. Pracownicy zobowiązani są do realizacji poszczególnych czynności przetwarzania zgodnie z zatwierdzonymi rejestrami, a wszelkie zmiany wpisów w rejestrach wymagają pisemnej zgody dyrektora II Liceum Ogólnokształcącego im. ppłk J. Modrzejewskiego w Jaśle.
8. W razie przetwarzania danych na podstawie zgody pracownik pozyskujący dane od osoby, której dotyczą zobowiązany jest uzyskać jej zgodę i spełnić wobec niej obowiązek informacyjny w imieniu Administratora.
9. W razie pozyskiwania danych od osoby, której dotyczą zobowiązany jest spełnić wobec niej obowiązek informacyjny w imieniu Administratora.
10. Administrator, uwzględniając ochronę danych w fazie projektowania, dokonuje analizy ryzyka przed rozpoczęciem przetwarzania (zgodnie z art.25 RODO).
11. Nie rzadziej niż raz w roku przeprowadzana jest analiza ryzyka utraty integralności, dostępności lub poufności informacji (na podstawie § 20 ust. 2 pkt 3 KRI w oparciu o podrozdział IV.13). Analiza ryzyka dotyczy czynności przetwarzania, które są opisane w Rejestrze czynności przetwarzania. Jeżeli Administrator przetwarza dane osobowe innego administratora, a umowa powierzenia nie stanowi inaczej analiza obejmuje również kategorie czynności przetwarzania.
12. Analiza ryzyka może być przeprowadzana po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne).
13. W razie stwierdzenia ryzyka mogącego mieć wpływ na bezpieczeństwo danych należy podjąć działania minimalizujące ryzyko.
14. W razie wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych przeprowadzana jest ocena skutków dla ochrony danych (na podstawie art. 35 RODO).

III.3 Standardy bezpieczeństwa danych przetwarzanych w formie tradycyjnej

1. Zadania wymagające przetwarzania danych osobowych realizują wyłącznie osoby upoważnione przez Administratora danych.
2. Dokumenty zawierające dane osobowe muszą być przechowywane w szafach zamykanych na klucz, a dostęp do nich mogą mieć wyłącznie osoby do tego uprawnione.
3. Klucze do szaf i pomieszczeń, gdzie przetwarza się dane osobowe są ewidencjonowane i mają do nich dostęp tylko uprawnione osoby.
4. Duplikaty kluczy do szaf i pomieszczeń, gdzie przechowywane są dane osobowe dorabia się wyłącznie na polecenie lub za zgodą Administratora danych.
5. Pracownik w czasie pracy powinien mieć na biurku tylko te dokumenty, które są mu potrzebne do realizacji określonego zadania.
6. W przypadku chwilowego opuszczenia stanowiska pracy dokumenty zawierające dane osobowe muszą być zabezpieczone przed dostępem osób nieuprawnionych.

7. Po zakończeniu pracy dokumenty muszą zabezpieczane w szafie zamykanej na klucz („zasada czystego biurka”).
8. Kopie robocze pism oraz inne przeznaczone do brakowania dokumenty, które zawierają dane osobowe, muszą być zniszczone w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w spełniającej ten wymóg niszczarce.
9. Dokumentacja zawierająca dane osobowe powinna być przechowywana w siedzibie administratora.
10. Przenoszenie dokumentacji poza siedzibę administratora dopuszczalne jest wyłącznie za wiedzą i zgodą Administratora lub gdy konieczność taka wynika z obowiązujących przepisów.

III.4 Standardy bezpieczeństwa danych przetwarzanych w systemie informatycznym

1. Oprogramowanie musi być aktualizowane na bieżąco.
2. Systemy operacyjne muszą być chronione przez programy antywirusowe.
3. Konto administracyjne musi być oddzielone od kont użytkowników - należy zapewnić ochronę plików systemowych (na podstawie § 20 ust. 2 pkt 12 e KRI).
4. Przed przystąpieniem do pracy pracownik zobowiązany jest sprawdzić czy stacja robocza, na której przetwarzane są dane osobowe nie ma śladów ingerencji osób trzecich.
5. Dane przetwarzane w systemie informatycznym chronione są przed nieuprawnionym dostępem. Pracownik zobligowany jest do przestrzeganie następujących zasad:
   - w czasie pracy należy mieć otwarte tylko te programy i aplikacje, które są potrzebne do realizacji określonego zadania,
   - w przypadku chwilowego opuszczenia stanowiska pracy należy wylogować się z systemu lub uruchomić wygaszacz ekranu zabezpieczony hasłem,
   - w razie przesyłania dokumentów z danymi osobowymi pocztą elektroniczną należy stosować mechanizmy kryptograficzne (hasła należy przekazać oddzielnym kanałem),
   - po zakończeniu pracy należy wylogować się z systemu,
   - po zakończeniu pracy wszelkie nośniki danych (dyski zewnętrzne, pendrivy, płyty CD) należy usunąć ze stacji roboczej i zabezpieczyć.
6. Należy stosować środki techniczne i organizacyjne oraz podejmować działania służące redukcji ryzyk, wynikających ze stwierdzonych podatności systemów informatycznych.
7. W razie dostrzeżenia nieujawnionych podatności systemów informatycznych mogących mieć wpływ na bezpieczeństwo danych należy niezwłocznie zgłosić to bezpośredniemu przełożonemu, Administratorowi danych lub Inspektorowi ochrony danych .
8. Nie rzadziej niż raz na pół roku należy przeprowadzić kontrolę zgodności systemów informatycznych z obowiązującymi normami prawnymi i regulacjami wewnętrznymi.
9. Nie rzadziej niż raz na rok należy przeprowadzić audyt wewnętrzny w zakresie bezpieczeństwa informacji (na podstawie § 20 ust. 2 pkt 14 KRI).
10. W określonych przepisami przypadkach, w szczególności związanych z przetwarzaniem danych z wykorzystaniem nowoczesnych technologii, przeprowadzana jest ocena skutków dla ochrony danych (zgodnie z art. 35 RODO).

III.5 Sankcje karne

1. Osoba, która przetwarza dane osobowe, których przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniona, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.
2. Jeżeli niedozwolone przetwarzanie dotyczy danych wrażliwych osoba, która dane przetwarza podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.
3. Osobie, która udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

Rozdział IV
PROCEDURY SŁUŻĄCE ZABEZPIECZENIU DANYCH

IV.1

UDZIELANIA DOSTĘPU DO DANYCH OSOBOWYCH

Podstawa prawna: § 20 ust. 2 pkt 4 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych i art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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

Cel: Określenie zasad dotyczących udzielania dostępu do danych osobowych.

Opis norm postępowania:

1. Osoba, która w związku z wykonywaniem obowiązków służbowych, przetwarza dane osobowe w imieniu administratora posiada pisemne upoważnienie (wzór upoważnienie określa załącznik nr 1).
2. Osoba, która nie jest upoważniona do przetwarzania danych, ale w związku z wykonywaniem obowiązków służbowych przebywa w pomieszczeniach, gdzie przetwarzane są dane osobowe posiada pisemne upoważnienie (wzór upoważnienie określa załącznik nr 2).
3. Upoważnienia wydaje Administrator danych (Dyrektor szkoły).
4. Upoważnienia są ewidencjonowane (wzór rejestru osób upoważnionych do przetwarzania danych osobowych określa załącznik nr 3, wzór rejestru osób upoważnionych do przebywania w pomieszczeniach, w których przetwarzane są dane osobowe określa załącznik nr 4).
5. Administrator danych może wyznaczyć pracownika szkoły do prowadzenia ewidencji wydanych upoważnień.
6. Osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznania się z przepisami RODO, Ustawy o ochronie danych osobowych oraz zasadami zawartymi w obowiązującej w szkole Polityce ochrony danych.

Załącznik Nr 1

Jasło, dnia ……..... r.

.....
(pieczęć Szkoły)

UPOWAŻNIENIE nr ……/20XX
do przetwarzania danych osobowych

Upoważniam Panią/Pana ..... zatrudnioną(ego) na stanowisku ..... w …… do przetwarzania danych osobowych w zakresie określonym w obowiązkach służbowych.

Niniejszym zobowiązuję Panią/Pana do zachowania w tajemnicy przetwarzanych danych osobowych oraz informacji o sposobie ich zabezpieczenia w czasie trwania umowy o pracę, a także po jej ustaniu

Upoważnienie obowiązuje od dnia..... 20…. r. i traci moc z chwilą odwołania lub rozwiązania / wygaśnięcia umowy o pracę.

.....
(pieczątka i podpis Administratora Danych)

OŚWIADCZENIE
o zachowaniu poufności i zapoznaniu się z przepisami

Oświadczam, że zostałem/am poinformowany/a o obowiązujących przepisach dotyczących przetwarzania danych osobowych i zobowiązuję się ich przestrzegać.

Oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz informacji o sposobie 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.

Jasło, dnia …… .....
(podpis pracownika)

Załącznik Nr 2

Jasło, dnia ……..... r.

.....
(pieczęć Szkoły)

UPOWAŻNIENIE nr ……/20XX
do przebywania w pomieszczeniach,
gdzie przetwarzane są dane osobowe

Upoważniam Panią/Pana ..... zatrudnioną(ego) na stanowisku ..... do przebywania w pomieszczeniach …….., w których przetwarzane są dane osobowe.

Niniejszym zobowiązuję Panią/Pana do zachowania w tajemnicy danych osobowych, do których może mieć Pani/Pan dostęp w związku z wykonywaniem obowiązków służbowych oraz informacji o sposobie ich zabezpieczenia zarówno w czasie trwania umowy o pracę jak i po jej ustaniu

Upoważnienie obowiązuje od dnia..... 20…. r. i traci moc z chwilą odwołania lub rozwiązania / wygaśnięcia umowy o pracę

.....
(pieczątka i podpis Administratora Danych)

OŚWIADCZENIE
o zachowaniu poufności i zapoznaniu się z przepisami

Oświadczam, że zostałem/am poinformowany/a o obowiązujących przepisach dotyczących przetwarzania danych osobowych i zobowiązuję się ich przestrzegać.

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

Jasło, dnia …… .....
(podpis pracownika)

Załącznik Nr 3

.....
(pieczęć Szkoły)

REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Stanowisko	Data nadania uprawnień i podpis ADO	Data odebrania uprawnień i podpis ADO	Uwagi

Załącznik Nr 4

.....
(pieczęć Szkoły)

REJESTR OSÓB UPOWAŻNIONYCH DO PRZEBYWANIA W POMIESZCZENIACH, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

L.p.	Imię i nazwisko	Stanowisko	Data nadania uprawnień i podpis ADO	Data odebrania uprawnień i podpis ADO	Uwagi

IV.2

ZABEZPIECZENIA URZĄDZEŃ SIECIOWYCH I SERWEROWYCH

Podstawa prawna: Art. 24 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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

Cel: Zapewnienie ochrony danych osobowych przetwarzanych w systemach informatycznych przed utratą lub nieuprawnionym dostępem.

Opis norm postępowania:

1. Urządzenia serwerowe zainstalowane są w szafie teleinformatycznej w pomieszczeniu, do którego dostęp mają wyłącznie osoby upoważnione przez Administratora danych.
2. W pomieszczeniu zapewnione muszą być zapewnione warunki zgodne z zaleceniami producenta poszczególnych urządzeń.
3. Urządzenia instalowane są w taki sposób, aby był zapewniony do nich swobodny dostęp fizyczny, w razie ich serwisowania bądź napraw.
4. Routery powinny być instalowane w takich miejscach, aby dostęp do nich miały tylko upoważnione osoby.
5. Urządzenia na których przetwarzane są dane powinny być podłączone pod system zasilania awaryjnego np. UPS, umożliwiającego podtrzymanie zasilania na czas konieczny do bezpiecznego wyłączenia urządzeń.
6. Okablowanie powinno być poprowadzone torami bezpiecznymi tj. podtynkowo, torem ziemnym lub w na ścianie w odpowiednich osłonach montażowych, zapewniających ochronę przed uszkodzeniem.
7. Okablowanie powinno być uporządkowane i oznakowane w sposób umożliwiający szybką identyfikację.

IV.3

ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

Podstawa prawna: § 21 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych i art. 24 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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

Cel: Zapewnienie ochrony przetwarzanych danych osobowych przed nieuprawnionym dostępem.

Opis norm postępowania:

1. System informatyczny musi posiadać ochronę antywirusową oraz zaporę sieciową, która obejmuje wszystkie stacje robocze oraz serwery.
2. Oprogramowanie powinno być skonfigurowane w sposób aby:
   - zapewnić automatyczne usuwanie wirusów, a w sytuacji kiedy nie jest to możliwe objęcie ich kwarantanną,
   - zapewnić okresowe skanowanie wszystkich dysków lokalnych oraz powiadamianie o wykrytym oprogramowaniu złośliwym.

IV.4

ZABEZPIECZENIA STACJI ROBOCZYCH

Podstawa prawna: Art. 24 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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

Cel: Zapewnienie ochrony przetwarzanych danych osobowych przed nieuprawnionym dostępem.

Opis norm postępowania:

1. Dostęp do pomieszczeń, gdzie znajdują się stacje robocze służące do przetwarzania danych powinny mieć wyłącznie osoby do tego upoważnione.
2. Stacje robocze muszą być zainstalowane i użytkowane w sposób zgodny z zaleceniami producenta – należy zapewnić dostęp powietrza (chłodzenie).
3. Okablowanie powinno być uporządkowane w sposób ograniczający możliwość przypadkowego rozłączenia.
4. Użytkownik nie powinien posiadać praw administracyjnych do stacji roboczej, chyba, że wymaga tego specyfika programów z których korzysta w związku z realizacją obowiązków służbowych.
5. Rozpoczęcie pracy w systemie zawsze wymaga logowania (wyklucza się możliwość autologowania).
6. W razie stwierdzenia znacznego ryzyka dostępu osób nieuprawnionych do danych przetwarzanych w systemie informatycznym w celu wzmocnienia zabezpieczeń stacji roboczych administrator może zalecić pracownikowi stosowanie
7. W czasie pracy ekran monitora musi być ustawiony w sposób uniemożliwiający wgląd w przetwarzane na nim dane osobom nieuprawnionym.
8. W przypadku bezczynności użytkownika uruchamiany jest automatycznie wygaszacz ekranu zabezpieczony hasłem. Czas po jakim uruchamiany jest wygaszacz należy dostosować indywidualnie przy uwzględnieniu specyfiki zadań danego pracownika, przy czym nie powinien on być dłuższy niż 10 minut.

IV.5

UDZIELANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

Podstawa prawna: § 20 ust. 2 pkt 4 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych i art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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

Cel: Zapewnienie prawidłowości i rozliczalności działań w systemie informatycznym.

Opis norm postępowania:

1. Uprawnienia do systemu może posiadać wyłącznie osoba, która korzysta z niego w związku z wykonywaniem obowiązków służbowych.
2. Uprawnienia do systemu nadaje Administrator systemu.
3. Przy nadawaniu dostępu stosuje się zasadę minimalizacji uprawnień, czyli przydzielanie ich w zakresie adekwatnym do wykonywanych zadań.
4. Nazwy kont (identyfikatory) muszą być unikalne i zapewniać jednoznaczną identyfikację osoby, która z niego korzysta. Identyfikator raz użyty nie może zostać wykorzystany ponownie.
5. Konto administratora systemu musi zapewniać rozliczalność działań oraz identyfikację osób z niego korzystających. Uprawnienia i hasła do konta administratora systemu nadaje Administrator Danych.
6. Metryki haseł do kont administratora systemu przechowywane są w zamkniętych kopertach w szafie pancernej, do której dostęp mają tylko uprawnione osoby.
7. Administrator systemu zobowiązany jest do bieżącej kontroli i weryfikacji zasadności nadanych użytkownikom uprawnień.
8. W razie stwierdzenia braku zasadności (np. zmiana zakresu obowiązków, rozwiązanie umowy o pracę) dostęp do systemu powinien być niezwłocznie cofnięty bądź zmodyfikowany.

IV.6

TWORZENIE I STOSOWANIE HASEŁ W SYSTEMIE INFORMATYCZNYM

Podstawa prawna: § 20 ust. 2 pkt 7 c Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych i art. 24 ust. 1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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

Cel: Zapewnienie ochrony systemu informatycznego w którym przetwarzane są dane osobowe przed nieuprawnionym dostępem.

Opis norm postępowania:

1. Hasło musi zawierać minimum 8 znaków, w tym małe i duże litery, przynajmniej jedną cyfrę i znak specjalny.
2. Hasło nie powinno zawierać danych użytkownika np. imion, nazwisk, daty urodzenia itp.
3. Hasło powinno być zmieniane nie rzadziej niż raz na 30 dni.
4. Hasło nie może być ujawnione innej osobie. W sytuacji podejrzenia, że taki fakt zaistniał hasło musi być natychmiast zmienione.
5. Hasła logowania do różnych systemów powinny być różne.
6. Hasło stosowane w systemie informatycznym szkoły nie może być wykorzystywane do innych celów np. zabezpieczenia zasobów prywatnych użytkownika.
7. Hasła startowe (generowane automatycznie podczas rejestracji konta użytkownika) należy zmienić przy pierwszym logowaniu.
8. Hasło powinno być wprowadzone w sposób maskowany.
9. Hasła nie mogą być przechowywane (np. zapisywane w pliku tekstowym lub w formie tradycyjnej) na stanowiskach pracy. Hasła użytkowników mogą zostać zdeponowane w bezpiecznym miejscu (np. sejfie, szafie pancernej) w zamkniętej i zapieczętowanej kopercie opisanej imieniem i nazwiskiem osoby, upoważnionej do jej otwarcia.

IV.7

PRZETWARZANIE DANYCH NA URZĄDZENIACH MOBILNYCH

Podstawa prawna: § 20 ust. 2 pkt 8 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych i art. 24 ust. 1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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

Cel: Zapewnienie bezpieczeństwa danych przetwarzanych na urządzeniach mobilnych.

Opis norm postępowania:

1. Dopuszczalne jest stosowanie usług chmurowych, co oznacza, że dane przechowywane są na serwerze podmiotu oferującego usługę, który odpowiada za dostępność do danych i zabezpieczenie serwera. Zawsze w takiej sytuacji wymagana jest umowa powierzenia danych, zawierająca przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora oraz obowiązki i prawa podmiotu przetwarzającego (zgodnie z art. 28 RODO).
2. Korzystanie z urządzeń mobilnych (w tym prywatnych) w celu przetwarzania danych osobowych jest dopuszczalne, ale wymaga stosowania wszystkich zabezpieczeń określonych w niniejszej polityce m.in.:
   - stosowanie programów antywirusowych,
   - stosowania haseł,
   - ochronę haseł przed dostępem osób nieuprawnionych (w tym niestosowanie autologowania),
   - zabezpieczenia dostępu do danych w razie utraty urządzenia (np. w wyniku kradzieży),
   - zapewnienie ochrony urządzenia przed nieuprawnionym dostępem (np. stosowanie wygaszaczy ekranu zabezpieczonych hasłem) lub jego utratą (stosowanie zasad dotyczących nośników danych).
3. Za właściwe zabezpieczenie służbowych urządzeń mobilnych odpowiedzialność ponosi Administrator danych.
4. Za właściwe zabezpieczenie prywatnych urządzeń mobilnych wykorzystywanych do przetwarzania danych odpowiedzialność ponosi pracownik.

IV.8

POSTĘPOWANIE Z NOŚNIKAMI DANYCH

Podstawa prawna: Art. 24 ust. 1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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

Cel: Zapewnienie ochrony przetwarzanych danych osobowych przed nieuprawnionym dostępem.

Opis norm postępowania:

1. Nośniki danych należy przechowywać w miejscu niedostępnym dla osób nieuprawnionych (np. w szafie pancernej).
2. Warunki środowiskowe przechowywania nośników danych muszą być zgodne z zaleceniami producentów tych urządzeń.
3. Przenoszenie nośników danych wymaga zabezpieczenia ich przed nieuprawnionym dostępem poprzez szyfrowanie lub pakowane w programie Zip oraz zabezpieczenie kodem. Kod musi być chroniony i zawierać minimum 8 znaków, w tym małe i duże litery, przynajmniej jedną cyfrę oraz znak specjalny.
4. Przenoszenie nośników danych powinno odbywać się z zachowaniem szczególnej uwagi i ostrożności. W przypadku zlecenia transportu nośników należy korzystać z usług sprawdzonych firm i kurierów.
5. Przenoszenie danych osobowych poza siedzibę Administratora dopuszczalne jest wyłącznie za jego wiedzą i zgodą.
6. Naprawa nośników danych powinna być przeprowadzona po trwałym usunięciu zapisanych na nim informacji lub jeżeli nie jest to możliwe zlecona podmiotowi, spełniającemu wymogi bezpieczeństwa, z którym zawarta została umowa powierzenia danych.
7. W celu odzyskania utraconych danych dopuszczalne jest za zgodą Administratora Danych przekazanie nośnika danych specjalistycznemu podmiotowi, spełniającemu wymogi bezpieczeństwa, z którym zawarta została umowa powierzenia danych.
8. Z nośników danych przeznaczonych do likwidacji należy trwale usunąć zapisane wcześniej dane lub uszkodzić je w taki sposób, aby odczyt danych stał się niemożliwy.

IV.9

ZARZĄDZANIE KOPIAMI ZAPASOWYMI

Podstawa prawna: Art. 24 ust. 1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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

Cel: Zapewnienie poufności, integralności i dostępności danych.

Opis norm postępowania:

1. Każdy pracownik przetwarzający dane osobowe zobowiązany jest do okresowego tworzenia kopii zapasowych.
2. Kopie zapasowe tworzone są w taki sposób, aby zapewnić dostępność danych w sytuacji awarii systemu.
3. Kopie zapasowe obejmują:
   - bazy danych gromadzonych w programach,
   - bazy danych gromadzonych w plikach i dokumentach.
4. Kopie należy wykonywać jako kopie plików.
5. Kopie można dodatkowo wykonywać jako „klonowanie" dysku lun jako obraz systemu. W celu zapewnienia prawidłowości odtworzenie obraz systemu trzeba wykonywać po każdej aktualizacji oprogramowania.
6. Kopie plików tworzone są raz w miesiącu, w ostatnim dniu roboczym. Odpowiedzialność za wykonanie kopii ponosi pracownik przetwarzający dane.
7. W celu zapewnienia prawidłowości działania kopii pracownik zobowiązany jest do sprawdzenia poprawności zapisu kopii zapasowych.
8. Nadzór nad wykonaniem kopii Administrator Danych lub osoba przez niego wyznaczona.\
9. Kopie zapasowe są oznaczone (data wykonania kopii i nazwisko osoby odpowiedzialnej) i przechowywane są w miejscu niedostępnym dla osób nieuprawnionych.

IV.10

PRZEGLĄDY I KONSERWACJE SYSTEMÓW

Podstawa prawna: § 20 ust. 2 pkt 10 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych i art. 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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

Cel: Zapewnienie prawidłowego działania systemów informatycznych przy utrzymaniu bezpieczeństwa przetwarzanych w nich danych osobowych.

Opis norm postępowania:

1. Przeglądy i konserwacje urządzeń wchodzących w skład systemów informatycznych wykonuje się zgodnie z zaleceniami ich producentów.
2. Prace serwisowe i naprawy powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
3. Bieżące naprawy przeprowadzają wyłącznie pracownicy lub inne osoby (np. zleceniobiorcy), które posiadają upoważnienie do przetwarzania danych osobowych.
4. Wszelkie prace związane z naprawami i konserwacją urządzeń, na których przetwarzane są dane osobowe, wymagające zaangażowania podmiotów zewnętrznych, odbywają się na podstawie umowy powierzenia, która winna zawierać przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora oraz obowiązki i prawa podmiotu przetwarzającego (zgodnie z art. 28 RODO).
5. Rozpoczęcie prac serwisowych wymaga zgody Administratora danych.
6. Przed rozpoczęciem prac przez osoby niebędące pracownikami II Liceum Ogólnokształcącego im. ppłk J. Modrzejewskiego w Jaśle należy dokonać potwierdzenia ich tożsamości.

IV.11

STOSOWANIE MONITORINGU WIZYJNEGO

Podstawa prawna: Art. 22^2 i art. 22^3 Ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2018 r. poz. 917 ze zmianami) i art. 108 a Ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz. U. z 2018 r. poz. 996, 1000 i 1290)

Cel: Ochrona danych przetwarzanych w związku ze stosowaniem monitoringu wizyjnego.

Opis norm postępowania:

1. Monitoring wizyjny stosowany jest w celu zapewnienia bezpieczeństwa uczniów i pracowników oraz ochrony mienia, w uzgodnieniu z organem prowadzącym, po przeprowadzeniu konsultacji z radą pedagogiczną, radą rodziców i samorządem uczniowskim.
2. Monitoring nie stanowi środka nadzoru nad jakością wykonywania pracy przez pracowników szkoły lub placówki.
3. Monitoring nie obejmuje pomieszczeń, w których odbywają się zajęcia dydaktyczne, wychowawcze i opiekuńcze, pomieszczeń, w których jest udzielana uczniom pomoc psychologiczno-pedagogiczna, pomieszczeń przeznaczonych do odpoczynku i rekreacji pracowników, pomieszczeń sanitarnohigienicznych, gabinetu profilaktyki zdrowotnej, szatni i przebieralni.
4. Opis środków technicznych i organizacyjnych zastosowanych celem zabezpieczenia gromadzonych w ten sposób danych określa Regulamin monitoringu wizyjnego ……., uzgodniony z organem prowadzącym szkołę.
5. Obowiązek informacyjny wobec osób objętych przebywających w obszarze objętym monitoringiem realizuje się poprzez stosowanie tablic informacyjnych, których treść określa regulamin.
6. Nagrania obrazu zawierające dane osobowe uczniów, pracowników i innych osób, których w wyniku tych nagrań można zidentyfikować, przetwarza się wyłącznie do celów, dla których zostały zebrane.
7. Po upływie okresu przechowywania, uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe uczniów, pracowników i innych osób, których w wyniku tych nagrań można zidentyfikować, podlegają zniszczeniu, o ile przepisy odrębne nie stanowią inaczej.
8. Dyrektor szkoły informuje uczniów i pracowników szkoły o wprowadzeniu monitoringu, poprzez ogłoszenia umieszczone na tablicach informacyjnych oraz stronie internetowej szkoły nie później niż 14 dni przed uruchomieniem monitoringu.
9. Dyrektor szkoły przed dopuszczeniem osoby do wykonywania obowiązków służbowych informuje ją na piśmie o stosowaniu monitoringu.

IV.12

UDOSTĘPNIANIE DANYCH

Podstawa prawna: Art. 24 ust. 1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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

Cel: Określenie warunków udostępniania danych.

Opis norm postępowania:

1. 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.
2. Udostępnienie danych może nastąpić na pisemny wniosek zawierający następujące elementy:
   - adresat wniosku (administrator danych),
   - wnioskodawca,
   - podstawa prawna (wskazanie potrzeby),
   - wskazanie przeznaczenia,
   - zakres informacji.
3. Administrator odmawia udostępnienia danych jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

IV.13 Analiza ryzyka

ANALIZA RYZYKA

Podstawa prawna: § 20 ust. 2 pkt 3 Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

Cel: Ocena ryzyka związanego z procesami przetwarzania danych i podjęcie działań adekwatnych do jego poziomu.

Opis norm postępowania:

Powołanie zespołu

1. Analizę ryzyka przeprowadza Administrator danych we współpracy z powołanym w tym celu zespołem zadaniowym.
2. W skład zespołu wchodzą pracownicy bezpośrednio zaangażowani w przetwarzanie danych.

Określenie zagrożeń

3. Zespół określa wykaz zagrożeń dla poszczególnych czynności i kategorii czynności. Uwzględniane są zagrożenia, których materializacja może spowodować naruszenie poufności, dostępności lub integralności przetwarzanych danych osobowych.
4. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zinwentaryzowanych czynności przetwarzania i kategorii czynności przetwarzania.

Wyznaczenie wartości ryzyka

5. Zespół szacuje prawdopodobieństwo (**P**) zmaterializowania zagrożenia dla poszczególnych czynności przetwarzania i kategorii czynności, według następujących kryteriów:

PRAWDOPODOBIEŃSTWO	CZĘSTOTLIWOŚĆ	SKALA (WAGA)
niskie	nie występuje lub występuje rzadziej niż raz w roku	P = 1
średnie	występuje kilka razy w roku	P = 2
wysokie	występuje co najmniej raz w tygodniu	P = 3

6. Zespół określa skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne, według następujących kryteriów:

POZIOM	SKUTKI WYSTĄPIENIA	SKALA (WAGA)
małe	nie powoduje naruszenia ochrony danych osobowych	S = 1
średnie	naruszenie, którego nie trzeba zgłaszać do organu nadzorczego	S = 2
duże	naruszenie danych szczególnych (wrażliwych) lub naruszenie dotykające dużej ilości osób, naruszenie podlegające zgłoszeniu do organu nadzorczego	S = 3

7. Korzystając z macierzy ryzyka, określa się wartość ryzyka dla poszczególnych zagrożeń jako: **N**(niską), **Ś** (średnią) lub **W** (wysoką)

	S=1	S=2	S=3
P=1	N	N	Ś
P=2	N	Ś	W
P=3	Ś	W	W

Postępowanie z ryzykiem

8. Na podstawie uzyskanych wyników Administrator decyduje o postępowaniu z ryzykiem. Reakcje na wartości ryzyka mogą być następujące:
   - **dla wartości N - akceptacja ryzyka**, czyli uznaje się, że zabezpieczenia są właściwe i nie ma potrzeby stosowania dodatkowych zabezpieczeń),
   - **dla wartości Ś - akceptacja ryzyka i monitorowanie**, czyli zakłada się, że zabezpieczenia są właściwe, ale wskazane jest stosowanie dodatkowych zabezpieczeń lub ich modyfikacja w miarę możliwości i dostępnych środków,
   - **dla wartości W - ryzyko nieakceptowalne**, oznacza, że zabezpieczenia są niewystarczające i należy podjąć działanie zmniejszające wartość ryzyka. Może to być:
     - przeniesienie, czyli przerzucenie ryzyka np. outsourcing, ubezpieczenie,
     - unikanie, czyli eliminacja działań powodujących ryzyko,
     - redukcja, czyli zastosowanie zabezpieczeń w celu obniżenia ryzyka.

     Zawsze gdy Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne . Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

IV.14

ZASADY ZGŁASZANIA NARUSZEŃ

Podstawa prawna: Art. 33 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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

Cel: Określenie zasad postępowania w razie zaistnienia naruszenia bezpieczeństwa danych.

Opis norm postępowania:

1. Każdy pracownik, który stwierdzi podatność, fakt naruszenia bezpieczeństwa danych, bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to bezpośredniemu przełożonemu, Administratorowi danych lub Inspektorowi ochrony danych.
2. W przypadku stwierdzenia naruszenia danych pracownik ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenie ochrony oraz ustalić przyczynę i sprawcę naruszenia ochrony.
3. W przypadku stwierdzenia naruszenia bezpieczeństwa danych nie należy podejmować działań mogących utrudnić określenie przyczyn wystąpienia incydentu i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratorowi danych lub Inspektora ochrony danych.
4. Administrator danych prowadzi postępowanie wyjaśniające w toku, którego:
   a) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki (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),
   b) inicjuje ewentualne działania dyscyplinarne,
   c) działa na rzecz przywrócenia działania jednostki po wystąpieniu incydentu,
   d) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze (wzór raportu z naruszenia określa załącznik nr 1).
6. W przypadku przetwarzania danych na podstawie umowy powierzenia o stwierdzeniu naruszenia zawiadamia się niezwłocznie Administratora danych..
7. W przypadku stwierdzenia, że naruszenie mogło skutkować naruszeniem praw i wolności osób fizycznych administrator zgłasza naruszenie do Urzędu Ochrony Danych nie później niż 72 godzin od stwierdzenia naruszenia (zgodnie z art.33 RODO).
8. W przypadku stwierdzenia, że incydent może powodować wysokie ryzyko naruszenie praw i wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o zaistniałym zdarzeniu (wzór zawiadomienia określa załącznik nr 2).

UWAGA! Przykłady naruszeń:

- zdarzenia losowe zewnętrzne - pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności;
- zdarzenia losowe wewnętrzne - awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych;
- umyślne incydenty - włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania.

Załącznik Nr 1

Jasło, dnia ……..... r.

.....
(pieczęć)

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Data incydentu: ..... r. Godzina incydentu: .....
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 Inspektora Ochrony Danych) *(podpis Administratora Danych)*

Załącznik Nr 2

Jasło, dnia ……..... r.

.....
(pieczęć)

Szanowna/y Pani/Pan

……

……

ZAWIADOMIENIE O NARUSZENIU OCHRONY DANYCH

Na podstawie art. 34 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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)

informuję o naruszeniu ochrony Pani/Pana danych osobowych

przetwarzanych przez ……

Charakter naruszenia	
Możliwe konsekwencje naruszenia	
Zastosowane/proponowane środki w celu zminimalizowania skutków naruszenia	

W razie pytań proszę o kontakt z Inspektorem Ochrony Danych - …….

tel. ……...…

.....
(podpis Administratora Danych)