Załącznik do Zarządzenia Dyrektora nr 5/2026

z dnia 17.06.2026 r.

SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

w Zespole Szkół Budowlanych w Rybniku

Czerwiec 2026

Wersja: 1.0

Do użytku wewnętrznego

Spis treści:

§ 1.

Słownik pojęć

Administrator - placówka reprezentowana przez dyrektora.

Administrator Systemu Informatycznego (ASI) - osoba zobowiązana do zarządzania systemem informatycznym (pracownik placówki lub zewnętrznej firmy/instytucji).

Dane osobowe - wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Osobą możliwą do zidentyfikowania jest taka osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak: imię, nazwisko, numer PESEL, dane adresowe, identyfikator internetowy, dane o lokalizacji, wizerunek albo jeden lub kilka czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby.

Dane szczególnej kategorii (tzw. dane wrażliwe) - dane osobowe ujawniające szczególnie chronione informacje o osobie, takie jak: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne służące jednoznacznej identyfikacji osoby, dane dotyczące zdrowia oraz życia seksualnego lub orientacji seksualnej.

Dyrektor - to osoba kierująca placówką, która reprezentuje placówkę na zewnątrz, dba o bezpieczeństwo i realizację celów edukacyjnych, przełożony służbowy pracowników.

Incydent bezpieczeństwa (incydent) - każde zdarzenie, które powoduje lub może powodować naruszenie poufności, integralności lub dostępności informacji.

Informacje/dane - każda treść tworzona, przechowywana lub przekazywana w placówce, (niezależnie od formy).

Inspektor Ochrony Danych (IOD) - osoba wyznaczona przez administratora do nadzorowania i zapewnienia przestrzegania przepisów o ochronie danych osobowych.

Naruszenie ochrony danych osobowych (naruszenie) - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Placówka – Zespół Szkół Budowlanych w Rybniku.

Przetwarzanie danych - jakiekolwiek operacje na danych osobowych, wykonywane w sposób zautomatyzowany lub niezautomatyzowany, takie 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 albo niszczenie.

RODO - 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).

Rodzic - rodzic, opiekun prawny oraz osoby (podmioty) sprawujące pieczę zastępczą nad dzieckiem.

System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur i narzędzi zastosowanych w celu przetwarzania informacji.

SZBI - System Zarządzania Bezpieczeństwem Informacji.

Uczeń - wychowanek, uczeń lub słuchacz uczęszczający do placówki.

UODO - Urząd Ochrony Danych Osobowych.

Upoważnienie - dokument potwierdzający legalny dostęp do danych osobowych.

Użytkownik - osoba upoważniona, która uzyskała uprawnienie do przetwarzania informacji lub korzystania z systemów informatycznych placówki.

---

§ 2.

Postanowienia ogólne SZBI

1. Cel ustanowienia SZBI

1) Niniejszy dokument ustanawia System Zarządzania Bezpieczeństwem Informacji w Zespole Szkół Budowlanych w Rybniku.
2) Celem SZBI jest:
   a) zapewnienie poufności, integralności i dostępności w procesach edukacyjnych, administracyjnych oraz technicznych,
   b) zapewnienie zgodności z RODO, ustawą o ochronie danych osobowych oraz innymi przepisami prawa,
   c) ograniczenie ryzyka wystąpienia incydentów bezpieczeństwa,
   d) zapewnienie ciągłości działania placówki w obszarze przetwarzania informacji,
   e) podnoszenie świadomości personelu w zakresie ochrony danych osobowych i informacji.
3) SZBI obejmuje w szczególności: politykę, procedury, wytyczne, zasady, instrukcje, rejestry i ewidencje oraz wzory i formularze.

2. Podstawa prawna

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO).
2) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.
3) Ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe.
4) Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy.
5) Ustawa z dnia 26 stycznia 1982 r. - Karta Nauczyciela.
6) Ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej.
7) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
8) Inne właściwe przepisy prawa powszechnie obowiązującego.

3. Zakres stosowania SZBI

1) SZBI stosuje się do wszystkich pracowników (bez względu na podstawę zatrudnienia), praktykantów, stażystów, wolontariuszy oraz podmiotów przetwarzających, którym powierzono dane placówki.
2) SZBI obejmuje informacje:
   a) w postaci papierowej,
   b) w systemach informatycznych,
   c) na nośnikach przenośnych oraz urządzeniach mobilnych,
   d) ustne i wizualne.
3) SZBI ma charakter wewnętrznego systemu zarządzania, przyjmowanego zarządzeniem dyrektora i podlega przeglądowi co najmniej raz w roku oraz każdorazowo w przypadku: istotnej zmiany przepisów prawa, istotnej zmiany infrastruktury IT, wystąpienia poważnego incydentu bezpieczeństwa. Zmiany SZBI są ogłaszane pracownikom w sposób zwyczajowo przyjęty w placówce - każde kolejne wydanie ma nadany numer wersji i prowadzona jest historia zmian.

4) Dla zapewnienia skuteczności wdrożonych zabezpieczeń, placówka prowadzi stały monitoring zgodności przetwarzania z prawem oraz SZBI. IOD planuje i przeprowadza okresowe audyty wybranych obszarów przetwarzania danych w placówce - minimum raz w roku. Wyniki oraz ewentualne zalecenia IOD są przekazywane dyrektorowi.
5) Wszyscy pracownicy i inne osoby objęte zakresem SZBI są zobowiązani do zapoznania się z jego treścią i potwierdzenia tego stosownym oświadczeniem (załącznik nr 1A lub 1B).
6) Osoby mające dostęp do informacji są świadome, że korzystanie z danych poza zakresem upoważnienia, ujawnianie ich osobom nieuprawnionym lub niestosowanie się do zapisów SZBI może skutkować odpowiedzialnością dyscyplinarną i prawną.
7) W przypadku kontroli ze strony organu nadzorczego (Prezesa UODO) lub audytu prowadzonego przez uprawnione organy (np. NIK, organ prowadzący), placówka zapewni pełną współpracę i udostępni wymaganą dokumentację wykazującą przestrzeganie przepisów (m.in. polityki, procedury, rejestry, umowy powierzenia).

4. Role i odpowiedzialność

1) **Dyrektor**:
   a) pełni funkcję administratora danych osobowych,
   b) zatwierdza SZBI i wprowadza go w życie,
   c) odpowiada za nadzór nad wdrożeniem i stosowaniem SZBI.
   d) zapewnia zasoby techniczne, organizacyjne i finansowe niezbędne do funkcjonowania SZBI,
   e) nadaje i odbiera upoważnienia do przetwarzania danych,
   f) zapewnia realizację praw osób, których dane dotyczą,
   g) powołuje Inspektora Ochrony Danych,
   h) nadzoruje działania podmiotów przetwarzających.
2) **Inspektor Ochrony Danych (IOD)**:
   a) monitoruje przestrzeganie przepisów o ochronie danych i niniejszego SZBI,
   b) doradza dyrektorowi i pracownikom w zakresie ochrony danych,
   c) opiniuje dokumenty związane z ochroną danych osobowych,
   d) projektuje rozwiązania służące wyeliminowaniu incydentów,
   e) przeprowadza audyty wewnętrzne w zakresie zgodności przetwarzania danych osobowych z przepisami,
   f) koordynuje obsługę incydentów dotyczących danych osobowych,
   g) współpracuje z organem nadzorczym oraz pełnieni funkcję punktu kontaktowego dla UODO,
   h) prowadzi szkolenia w zakresie ochrony danych osobowych oraz zagrożeń związanych z ich przetwarzaniem,
   i) pełnieni funkcję punktu kontaktowego dla osób, których dane dotyczą.
   j) ma dostęp do pomieszczeń, w których zlokalizowane są przetwarzane dane, celem przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w zakresie oceny zgodności przetwarzania danych z przepisami prawa,
   k) uzyskuje pisemne lub ustne wyjaśnienia w zakresie niezbędnym do ustalenia stanu faktycznego,
   l) ma prawo dostępu do dokumentów, urządzeń, nośników, systemów informatycznych oraz wszelkich danych mających bezpośredni związek

z problematyką przeprowadzanego audytu zgodności przetwarzania danych z przepisami prawa,

3) **Administrator Systemu Informatycznego (ASI):**
   a) odpowiada za funkcjonowanie i bezpieczeństwo systemów IT,
   b) wdraża i utrzymuje techniczne środki bezpieczeństwa,
   c) zarządza kontami i uprawnieniami w systemach,
   d) udziela użytkownikom wsparcia technicznego,
   e) wykonuje kopie zapasowe i testy odtwarzania,
   f) prowadzi rejestry zasobów,
   g) monitoruje działanie systemów i zgłasza podejrzane działania.
4) **Pracownicy, współpracownicy, praktykanci, stażyści, wolontariusze:**
   a) są zobowiązani do przestrzegania przepisów prawa i SZBI,
   b) przetwarzają informacje zgodnie z zakresem powierzonych obowiązków i wyłącznie w granicach nadanego upoważnienia,
   c) dbają o bezpieczeństwo danych w dokumentacji papierowej i elektronicznej oraz chronią informacje przed dostępem osób nieuprawnionych,
   d) niezwłocznie zgłaszają incydenty bezpieczeństwa.
5) **Podmioty przetwarzające**:
   a) działają wyłącznie na podstawie umów powierzenia przetwarzania danych osobowych,
   b) spełniają minimalne wymagania bezpieczeństwa określone w umowie i w niniejszym SZBI.

---

§ 3.

Polityka Bezpieczeństwa Informacji

1. Postanowienia ogólne

1) Polityka obejmuje wszystkie systemy informacyjne, dokumentację papierową i elektroniczną, środki komunikacji i infrastrukturę IT placówki.
2) Polityka obejmuje wszelkie informacje przetwarzane w placówce, w szczególności:
   a) dane osobowe uczniów, rodziców, pracowników i innych osób,
   b) informacje związane z realizacją zadań dydaktycznych, wychowawczych i opiekuńczych,
   c) informacje kadrowe, finansowe, organizacyjne i techniczne.

2. Zasady ogólne bezpieczeństwa informacji

1) W placówce stosuje się następujące zasady:
   a) **legalności, rzetelności i przejrzystości** - informacje są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą,
   b) **poufności** - informacje udostępnia się wyłącznie osobom uprawnionym,
   c) **integralności** - informacje są chronione przed nieuprawnioną modyfikacją,
   d) **dostępności** - informacje są dostępne dla osób uprawnionych wtedy, gdy jest to niezbędne do realizacji zadań,
   e) **odporności** - środki techniczne i organizacyjne są dobierane proporcjonalnie do poziomu ryzyka związanego z danym zasobem,

f) **rozliczalności** - działania na informacjach są dokumentowane w sposób umożliwiający wykazanie zgodności z przepisami,

g) **ograniczenia celu** - dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach,

h) **minimalizacji** - gromadzone i przetwarzane są tylko takie dane osobowe, które są niezbędne do osiągnięcia określonych celów wynikających z przepisów prawa lub zgody osoby fizycznej. Zakres przetwarzanych danych jest ograniczony do minimum wymaganego dla danego zadania. Obowiązuje zakaz przetwarzania danych „na zapas" lub w szerszym zakresie niż cel tego wymaga,

i) **prawidłowości** - dane osobowe są poprawne i w razie potrzeby uaktualniane,

j) **ograniczenia przechowywania** - dane osobowe przechowywane są w formie umożliwiającej identyfikację osób tylko tak długo, jak to konieczne do realizacji celu,

k) **czystego biurka** - dokumenty i jakiekolwiek nośniki informacji (płyty CD, DVD, pamięci flash, USB itp.) przechowywane są poza zasięgiem wzroku i dłoni osób nieupoważnionych oraz nie są pozostawiane bez nadzoru,

l) **czystego ekranu** - uniemożliwienie dostępu osobom nieupoważnionym do informacji wyświetlanych na ekranie i blokowanie urządzenia przed odejściem od stanowiska (np. skrót klawiszowy Windows+L),

m) **czystej drukarki** - natychmiastowe zabieranie dokumentów z urządzeń drukujących po ich wydrukowaniu, zeskanowaniu czy skserowaniu,

n) **czystego kosza** - trwałe niszczenie niepotrzebnych dokumentów, brudnopisów, zbędnych kopii, a także nośników, zamiast wyrzucania ich do kosza na śmieci,

o) **czystej tablicy** - pracownicy nie zamieszczają na tablicach (w salach, biurach) informacji podlegających ochronie.

3. Klasyfikacja informacji

1) Celem klasyfikacji informacji jest wprowadzenie jednolitych zasad oznaczania, ochrony i gospodarowania informacjami, aby zapewnić właściwy poziom ochrony.

2) Każda informacja ma właściciela - dyrektora lub upoważnioną osobę, która odpowiada za klasyfikację informacji, decyzję o jej udostępnieniu i zapewnienie adekwatnych środków ochrony.

3) Każda informacja powinna mieć przypisaną kategorię w chwili jej tworzenia lub pozyskania. Klasyfikacji dokonuje twórca informacji lub właściciel zasobu informacyjnego.

4) Oznaczenie kategorii odbywa się poprzez:

   a) dokument papierowy - oznaczenie poziomu klasyfikacji w nagłówku, stopce, teczce lub segregatorze,

   b) dokument elektroniczny - oznaczenie poziomu klasyfikacji w nagłówku, stopce, nazwie pliku, folderu lub metadanych.

5) Informacje w placówce klasyfikuje się w następujące kategorie:

   a) **Informacje publiczne (jawne):**

      i. Informacje podlegające udostępnieniu na podstawie m.in. przepisów o dostępie do informacji publicznej, np.:

         - statut placówki,
         - regulaminy,
         - dokumenty organizacyjne (np. kalendarz roku szkolnego),
         - ogłoszenia na stronie internetowej.

ii. Ochrona podstawowa:
- brak konieczności zabezpieczania przed ujawnieniem,
- wymagane zabezpieczenia integralności i dostępności.

iii. Nie wymagają oznaczenia.

b) **Informacje wewnętrzne:**

i. Informacje przeznaczone wyłącznie dla osób zatrudnionych lub współpracujących z placówką, których ujawnienie mogłoby negatywnie wpłynąć na funkcjonowanie placówki, np.:
- wewnętrzna korespondencja służbowa,
- projekty dokumentów, notatki,
- wewnętrzne ustalenia.

ii. Ochrona:
- przechowywanie w miejscach niedostępnych dla osób postronnych,
- nie są udostępniane poza placówkę bez zgody dyrektora.

iii. Oznaczanie informacji: „Do użytku wewnętrznego".

c) **Informacje poufne:**

i. Informacje wymagające szczególnej ochrony - w tym dane osobowe uczniów, rodziców, pracowników, dane szczególnej kategorii, dane finansowe, dokumenty kadrowe, informacje o bezpieczeństwie placówki, dane z monitoringu, np.:
- dziennik elektroniczny i zawarte w nim dane,
- dokumentacja przebiegu nauczania, działalności wychowawczej i opiekuńczej,
- orzeczenia PPP, opinie psychologiczne,
- dokumenty płacowe, kadrowe i socjalne,
- nagrania z monitoringu,
- zbiory danych archiwalnych,
- hasła, klucze kryptograficzne, konfiguracje IT.

ii. Ochrona:
- dostęp tylko dla osób upoważnionych,
- są zabezpieczone fizycznie, organizacyjnie i technicznie (m.in. hasła, szyfrowanie, kontrola dostępu, przechowywanie w zamkniętych szafach, chronionych pomieszczeniach lub zabezpieczonych systemach IT),
- ich udostępnienie wymaga podstawy prawnej.

iii. Oznaczanie informacji: „POUFNE".

4. Przechowywanie i niszczenie informacji

1) Informacje przechowywane są zgodnie z przepisami prawa i wymaganiami archiwalnymi m.in.:
   a) Jednolitym Rzeczowym Wykazie Akt,
   b) przepisami o archiwum,
   c) przepisami oświatowymi.
2) Po upływie okresu przechowywania dane podlegają usunięciu, anonimizacji lub przekazaniu do archiwum zgodnie z obowiązującymi przepisami.

3) Niszczenie odbywa się w sposób uniemożliwiający odtworzenie:
   a) papier (szczególnie dokumenty poufne) - w niszczarkach ścinkowych klasy P-4 lub wyższej,
   b) nośniki elektroniczne - trwałe kasowanie poprzez nadpisywanie, demagnetyzację lub fizyczne zniszczenie,
4) W przypadku brakowania dokumentacji masowej powołuje się komisję, która dokonuje przeglądu i kwalifikacji akt.
5) Zniszczenie informacji dokumentuje się protokołem (załącznik nr 14A) oraz wpisuje do Rejestru niszczenia dokumentów i nośników danych (załącznik nr 14B).
6) Przegląd dokumentacji do zniszczenia odbywa się co najmniej raz w roku.

---

§ 4.

Przetwarzanie Danych Osobowych

1. Cele przetwarzania

1) Dane osobowe przetwarzane są w szczególności w celu:
   a) realizacji zadań wynikających z przepisów prawa oświatowego,
   b) realizacji zadań dydaktycznych, wychowawczych i opiekuńczych,
   c) prowadzenia dokumentacji przebiegu nauczania i wychowania,
   d) pomocy psychologiczno-pedagogicznej,
   e) organizacji konkursów, wycieczek, projektów i innych form działalności placówki,
   f) realizacji zadań kadrowo-płacowych i administracyjnych,
   g) obsługi świadczeń socjalnych, stypendiów,
   h) zapewnienia bezpieczeństwa uczniów, pracowników i mienia placówki,
   i) komunikacji i promocji działalności.

2. Podstawy prawne przetwarzania

1) Przetwarzanie danych osobowych jest zgodne z prawem wyłącznie w przypadkach, gdy spełniony jest co najmniej jeden z poniższych warunków:
   a) 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 (art. 6 ust. 1 lit. b RODO),
   b) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c RODO),
   c) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej (art. 6 ust. 1 lit. e RODO),
   d) przetwarzanie jest niezbędne do ochrony żywotnych interesów (ochrony życia i zdrowia) osoby, której dane dotyczą, lub innej osoby fizycznej (art. 6 ust. 1 lit. d RODO),
   e) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów (art. 6 ust. 1 lit. a RODO).
2) Dane szczególnych kategorii przetwarza się zgodnie z art. 9 RODO, m.in. gdy jest to niezbędne do realizacji obowiązków w zakresie oświaty i ochrony zdrowia.

3) Przetwarzanie danych dzieci odbywa się z poszanowaniem zasady szczególnej ochrony małoletnich wynikającej z RODO oraz wytycznych Europejskiej Rady Ochrony Danych.

3. Kategorie danych osobowych przetwarzanych w placówce

1) Placówka może przetwarzać dane osobowe:
   a) **Uczniów**, w tym:
      - imię, nazwisko, datę urodzenia, PESEL, adres zamieszkania,
      - dane rodziców/opiekunów prawnych,
      - oceny, wyniki klasyfikacji, frekwencję,
      - dane o stanie zdrowia,
      - dane wrażliwe w dokumentacji psychologiczno-pedagogicznej,
      - wizerunek.
   b) **Rodziców i opiekunów prawnych**, w tym:
      - dane kontaktowe,
      - informacje niezbędne do realizacji obowiązków placówki.
   c) **Pracowników**, w tym:
      - dane kadrowe, płacowe, socjalne,
      - dane wrażliwe (np. zaświadczenie o niekaralności, orzeczenia lekarskie).
   d) **Gości i interesantów**, w tym:
      - dane identyfikacyjne przy wejściu na teren placówki,
      - wizerunek w systemie monitoringu.

4. Realizacja obowiązku informacyjnego

1) Placówka realizuje obowiązek informacyjny w formie:
   a) pisemnych klauzul informacyjnych (załącznik nr 4A/B/itd.),
   b) informacji zamieszczonych na stronie internetowej placówki i BIP,
   c) informacji dostępnych w sekretariacie i na tablicach ogłoszeń,
   d) klauzul dołączanych do dokumentacji np. rekrutacyjnej, kadrowej, wydarzeń i zgód.
2) Terminy realizacji:
   a) bezpośrednie pozyskanie danych - informacja w momencie zbierania danych (art. 13 RODO),
   b) dane z innego źródła - informacja w ciągu 30 dni, najpóźniej przy pierwszym kontakcie (art. 14 RODO).
3) Treść klauzul informacyjnych zawiera:
   a) dane administratora,
   b) dane kontaktowe IOD,
   c) cele i podstawy prawne przetwarzania,
   d) odbiorców danych,
   e) okres przechowywania,
   f) prawa osób, których dane dotyczą,
   g) informację o planowanym transferze poza Europejski Obszar Gospodarczy,
   h) źródło danych (dla art. 14 RODO).

4) Dopuszcza się warstwowe przekazywanie informacji polegające na wskazaniu osobie, której dane dotyczą, jedynie najistotniejszych elementów, odsyłając jednocześnie do pełnej treści obowiązku informacyjnego, np. na stronie internetowej. Takie rozwiązanie jest dopuszczalne w przypadku, gdy administrator z uwagi na kontekst przetwarzania danych oraz narzędzia komunikacji nie ma możliwości, żeby wykonać w pełni obowiązek informacyjny lub byłoby to utrudnione (np. zaproszenie na wydarzenia).

5. Udostępnianie danych osobowych

1) Dane osobowe mogą być udostępniane podmiotom zewnętrznym wyłącznie na podstawie przepisów prawa i pisemnego wniosku podmiotu uprawnionego - tylko w zakresie niezbędnym do spełnienia obowiązku ciążącego na administratorze. Odbiorca używa ich do własnych, odrębnych celów, stając się samodzielnym administratorem danych.
2) Przed udostępnieniem danych należy upewnić się co do tożsamości wnioskującego oraz podstawy prawnej. W wątpliwych sytuacjach zasięgana jest opinia IOD.
3) Typowi odbiorcy to:
   a) Urząd Miasta Rybnika jako organ prowadzący - nadzór finansowy, sprawozdawczość, arkusz organizacyjny, audyt wewnętrzny,
   b) Kuratorium Oświaty - nadzór pedagogiczny,
   c) Okręgowa Komisja Egzaminacyjna - organizacja i przeprowadzenie egzaminów,
   d) Ministerstwo Edukacji Narodowej - zgodnie z ustawą o Systemie Informacji Oświatowej,
   e) ZUS i Urząd Skarbowy - obowiązki płatnika,
   f) banki - wypłata wynagrodzeń,
   g) inna jednostka oświatowa - przekazanie dokumentacji ucznia w związku ze zmianą jednostki,
   h) Policja, sądy, OPS - żądanie ma konkretną podstawę prawną i jest ograniczone do niezbędności.
4) Każdorazowo udostępnienie danych na żądanie jest dokumentowane w Rejestrze udostępnień danych (załącznik nr 5) ze wskazaniem komu, jakie dane i na jakiej podstawie przekazano.

6. Powierzanie przetwarzania danych osobowych

1) Dane osobowe mogą być powierzone podmiotom zewnętrznym na podstawie pisemnej Umowy powierzenia przetwarzania danych osobowych (załącznik nr 6A). Podmiot przetwarzający (procesor) wykonuje usługę dla administratora, przetwarzając dane w jego imieniu, na jego rzecz i zgodnie z jego instrukcjami.
2) Administrator może powierzać przetwarzanie danych wyłącznie podmiotom zapewniającym odpowiednie gwarancje bezpieczeństwa, co wiąże się z koniecznością weryfikacji podmiotu przetwarzającego pod kątem stosowanych środków technicznych i organizacyjnych dla ochrony danych osobowych (załącznik nr 6B).
3) Dopuszcza się możliwość zawarcia umowy powierzenia na wzorze zaproponowanym przez podmiot przetwarzający, pod warunkiem posiadania wymaganych zapisów, w szczególności:
   a) przedmiotu i czasu trwania,
   b) charakteru i celu przetwarzania,
   c) rodzaju danych i kategorii osób,
   d) obowiązków administratora i procesora,

e) zachowania poufności,
f) środków bezpieczeństwa,
g) zasad korzystania z podprocesorów,
h) pomocy w realizacji praw osób,
i) obowiązku zgłaszania naruszeń bez zbędnej zwłoki,
j) wsparcia przy wykazaniu zgodności z RODO,
k) usunięcia/zwrotu danych po zakończeniu,
l) umożliwienia audytu.

4) Typowe usługi, w których następuje powierzenie danych osobowych to:
a) dziennik elektroniczny,
b) platforma edukacyjna (Microsoft 365, Google Workspace),
c) hosting strony internetowej,
d) wydruk legitymacji,
e) niszczenie dokumentów przez firmę zewnętrzną,
f) system monitoringu wizyjnego (gdy zapis jest realizowany na obcym serwerze, serwis),
g) firma ochroniarska (jeśli monitoring jest przez nią nadzorowany),
h) serwis i usługi IT.

5) Każda zawarta umowa powierzenia przetwarzania danych osobowych zostaje wpisana do Rejestru umów powierzenia (załącznik nr 6C).

6) Co do zasady placówka nie przekazuje danych osobowych poza Europejski Obszar Gospodarczy. Jeżeli jednak konieczne jest takie działanie to zapewnione muszą być odpowiednie zabezpieczenia zgodnie z Rozdziałem V RODO np. decyzja Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony, standardowe klauzule umowne czy wiążące reguły korporacyjne.

7. Prawa osób, których dane dotyczą

1) Osobie, której dane dotyczą (np. uczeń, rodzic, opiekun, pracownik), przysługuje prawo:
a) **dostępu do danych** - potwierdzenie czy dane są przetwarzane, a jeśli tak, to przekazanie kopii tych danych,
b) **sprostowania danych** - niezwłoczna weryfikacja i korekta błędnych danych we wszystkich miejscach ich przetwarzania,
c) **usunięcia danych** („prawo do bycia zapomnianym") - usunięcie danych bez zbędnej zwłoki, jeśli ich przetwarzanie nie wynika z obowiązku prawnego placówki,
d) **ograniczenia przetwarzania** - do czasu oceny prawidłowości danych lub zgodności przetwarzania z prawem możliwe jest wyłącznie ich przechowywanie,
e) **sprzeciwu** - zaprzestanie przetwarzania, gdy szczególna sytuacja danej osoby, jej interesy, prawa i wolności przeważają nad realizacją zadania publicznego,
f) **przenoszenia danych** - prawdopodobnie nie wystąpi w placówce, ponieważ dotyczy danych przetwarzanych automatycznie na podstawie zgody lub umowy,
g) **wycofania zgody** - zakończenie przetwarzania danych, które były wykorzystywane na podstawie wcześniej wyrażonej zgody,
h) **wniesienia skargi** do Prezesa UODO - uznanie, że przetwarzanie danych narusza przepisy RODO.

2) Procedura obsługi wniosków osób, których dane dotyczą:

a) wniosek może być złożony w placówce lub u IOD - pisemnie, elektronicznie lub osobiście. Każdy pracownik, który odbierze wniosek tego typu, ma obowiązek niezwłocznie przekazać go do dyrektora oraz IOD,

b) wnioski realizowane są przez administratora we współpracy z IOD i są wolne od opłat, z zastrzeżeniem wyjątków określonych w przepisach prawa,

c) każdy otrzymany wniosek jest ewidencjonowany w Rejestrze żądań (załącznik nr 7A),

d) w przypadku uzasadnionych wątpliwości co do tożsamości osoby fizycznej składającej wniosek, można zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą. Przy wniosku otrzymanym elektronicznie można poprosić o dodatkowe uwierzytelnienie np. podanie szczególnej informacji, którą również posiada placówka lub poprosić o stawienie się osobiście. Jeśli wniosek jest składany przez opiekuna w sprawie danych dziecka, placówka weryfikuje posiadanie władzy rodzicielskiej albo prawa do opieki (na podstawie posiadanych akt),

e) analiza treści wniosku:

- jakich danych dotyczy,
- w jakich zbiorach/systemach dane się znajdują,
- podstawa prawna i zakres możliwej realizacji,
- jeśli jest niejasna lub zbyt ogólna, kontakt z wnioskodawcą celem doprecyzowania,

f) realizacja żądania bądź odmowa,

g) administrator udziela odpowiedzi bez zbędnej zwłoki w terminie maksymalnie 1 miesiąca od otrzymania wniosku. Jeśli charakter sprawy jest skomplikowany, termin można przedłużyć o kolejne 2 miesiące, ale należy w ciągu pierwszego miesiąca poinformować wnioskodawcę o przedłużeniu terminu i jego powodach. Odpowiedź powinna być udzielona tą samą drogą, jaką przyszło żądanie, chyba że wnioskodawca zażądał innej. Odpowiedzi udziela się zgodnie z zatwierdzonym szablonem (załącznik nr 7B).

8. Nadawanie, zmiana i odbieranie upoważnień do przetwarzania danych

1) Dostęp do danych osobowych w placówce mają wyłącznie osoby upoważnione przez administratora. Każdy pracownik lub inna osoba przed rozpoczęciem przetwarzania danych otrzymuje imienne upoważnienie wskazujące zakres danych i czynności do jakich jest uprawniony. Przyjmuje się zasadę, że dostęp ma być ograniczony do niezbędnego minimum. Upoważnienia nadaje i odwołuje dyrektor w formie pisemnej (załącznik nr 3A).
2) Dostęp do dokumentacji Zakładowego Funduszu Świadczeń Socjalnych wymaga odrębnego upoważnienia (załącznik nr 3B).
3) Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych oraz sposobów ich zabezpieczenia, co potwierdza podpisując stosowne oświadczenie o zachowaniu poufności (załącznik nr 2A lub 2B) oraz zapoznaniu się z niniejszym SZBI.
4) Każde upoważnienie otrzymuje unikalny numer i jest wpisywane do Rejestru upoważnień (załącznik nr 3C). Oryginał upoważnienia przechowuje się w aktach kadrowych lub w oddzielnym segregatorze.
5) Przy zmianie stanowiska lub zakresu obowiązków upoważnienie do przetwarzania danych jest aktualizowane odpowiednio do nowych potrzeb. Czynności te dokumentuje się w Rejestrze upoważnień.

6) W przypadku zakończenia zatrudnienia lub współpracy, dyrektor formalnie odwołuje upoważnienie do przetwarzania danych poprzez umieszczenie odpowiedniej adnotacji na upoważnieniu (np. „upoważnienie wygasa z dniem ... z powodu zakończenia zatrudnienia") oraz w Rejestrze upoważnień.
7) Administrator dokonuje raz w roku okresowego przeglądu wszystkich aktywnych upoważnień. Sprawdza czy dane osoby nadal pracują, czy zakres uprawnień jest adekwatny do bieżących zadań oraz czy nie ma osób przetwarzających dane bez formalnego upoważnienia.
8) W przypadku stwierdzenia nadużycia uprawnień, dostęp może być natychmiast zawieszony, a sprawa skierowana do postępowania wyjaśniającego przez dyrektora i IOD.

9. Anonimizacja i pseudonimizacja

1) Celem stosowania anonimizacji i pseudonimizacji jest:
   a) ograniczenie ryzyka naruszenia ochrony danych osobowych,
   b) realizacja zasady minimalizacji danych,
   c) zwiększenie bezpieczeństwa przetwarzania informacji,
   d) umożliwienie legalnego wykorzystywania danych do celów statystycznych, sprawozdawczych i organizacyjnych.
2) Anonimizacja i pseudonimizacja są standardowymi środkami bezpieczeństwa informacji. Ich stosowanie jest obowiązkowe, gdy dane nie są potrzebne w pełnej postaci lub można osiągnąć cel przetwarzania przy mniejszej ilości danych osobowych.
3) Anonimizacja to proces przetworzenia danych osobowych w sposób trwały i nieodwracalny, który uniemożliwia odtworzenie tożsamości osób, których dane dotyczą. Po anonimizacji:
   a) nie da się ustalić, kogo dane dotyczą,
   b) nikt (także administrator) nie jest w stanie przywrócić tożsamości osoby,
   c) dane przestają być danymi osobowymi w rozumieniu RODO. Niewłaściwe zanonimizowanie (np. podanie imienia i pierwszej litery nazwiska) może umożliwić identyfikację i jest naruszeniem zasad ochrony danych.
4) Przykłady metod anonimizacji:
   a) usunięcie identyfikatorów bezpośrednich i pośrednich (np. usunięcie lub zamiana imion i nazwisk na przypadkowe symbole),
   b) generalizacja danych (np. zamiana daty urodzenia na przedział wiekowy),
   c) grupowanie danych (np. wyniki prezentowane statystycznie),
   d) zaczernienie tekstu lub obrazów przed wykonaniem papierowej kopii dokumentów,
   e) zaczernienie tekstu w dokumentach elektronicznych w sposób uniemożliwiający cofnięcie zmiany np. zastosowanie narzędzi, które umożliwiają trwałe zaczernienie w plikach PDF lub dokumenty wydrukować, zanonimizować (zaczernić), a następnie zeskanować,
   f) zniekształcenie obrazu (w przypadku wizerunku) lub głosu osoby fizycznej,
   g) usunięcie metadanych, czyli ustrukturyzowanych informacji opisujących plik np. autor i lokalizacja GPS w zdjęciach.
5) Przykłady sytuacji i procesów podlegających anonimizacji:
   a) raporty i analizy - tworząc raporty wewnętrzne (np. statystyki), pracownicy korzystają z danych poddanych anonimizacji, usuwają imiona/nazwiska i przedstawiają wyniki jako ogólne zestawienia liczbowe. Dzięki temu raporty

pozwalają ocenić osiągnięcia całych grup bez ujawniania indywidualnych tożsamości,

b) udostępnianie informacji publicznej - przy udostępnianiu dokumentów (np. sprawozdań z rady pedagogicznej) należy anonimizować wszelkie dane, które pozwalają zidentyfikować osoby fizyczne (np. uczniów, rodziców, pracowników innych niż nauczyciele) oraz dane niezwiązane z pełnieniem funkcji publicznych osób występujących w takiej roli,

c) publikacja informacji w BIP - przy publikacji dokumentów w Biuletynie Informacji Publicznej (np. protokołów z kontroli Kuratorium Oświaty) należy anonimizować wszelkie dane, które pozwalają zidentyfikować osoby fizyczne. Pozostawia się dane osób pełniących funkcje publiczne mające związek z wykonywaniem zadań publicznych (np. imię i nazwisko wizytatora/kontrolującego, dyrektora).

6) Pseudonimizacja to proces przetworzenia danych osobowych w taki sposób, że dane nie mogą być przypisane konkretnej osobie bez użycia dodatkowych, odrębnie przechowywanych informacji. W przeciwieństwie do anonimizacji, pseudonimizacja jest procesem odwracalnym. Dane spseudonimizowane pozostają danymi osobowymi i podlegają ochronie prawnej tak długo, jak można je powiązać z osobą fizyczną przy użyciu dodatkowych informacji (klucza).

7) Przykłady metod pseudonimizacji:

a) numeracja - zastępowanie danymi technicznymi (np. Uczeń_001, nr kadrowy) i przechowywanie tabeli powiązań w odrębnym miejscu,

b) tokenizacja - zastąpienie losowymi identyfikatorami (np. ID1768, numer klienta) i przechowywanie tabeli powiązań w odrębnym miejscu,

c) szyfrowanie - zabezpieczenie danych kluczem/hasłem, który jest przechowywany osobno.

8) Przykłady sytuacji i procesów podlegających pseudonimizacji:

a) badania - jeżeli placówka prowadzi badania edukacyjne lub współpracuje z uczelniami, może przekazywać dane spseudonimizowane (przypisuje uczniom kody zamiast nazwisk). Dodatkowe dane (mapujące kody na osoby) przechowywane są tylko u administratora,

b) rejestry i zestawienia - gdy identyfikacja osób nie jest konieczna,

c) ograniczenie identyfikacji osób dla części pracowników lub wykonawców - przy zachowaniu możliwości przypisania danych do osoby w uzasadnionych przypadkach (np. realizacja praw osoby, korekta, bezpieczeństwo).

9) Sprawdzenie skuteczności anonimizacji i pseudonimizacji obejmuje:

a) weryfikację identyfikatorów bezpośrednich (np. imię, nazwisko, adres),

b) analizę identyfikatorów pośrednich i kontekstu (np. unikatowe cechy, opisy zdarzeń, cechy pozwalające na identyfikację w społeczności lokalnej, charakter pisma),

c) sprawdzenie czy połączenie dostępnych informacji z innymi publicznymi zbiorami umożliwia identyfikację,

d) sprawdzenie metadanych i warstw dokumentu (np. warstwa tekstowa w PDF, historia zmian, komentarze),

e) kontrolę wtórną (weryfikacja przez drugą upoważnioną osobę przed publikacją/udostępnieniem).

10. Wykorzystanie wizerunku i danych osobowych

1) Wizerunek jest jedną z danych osobowych, a także dobrem osobistym, zatem podlega również ochronie na podstawie przepisów zawartych w Kodeksie cywilnym. Jest to prawo niemajątkowe, niezbywalne, przysługujące każdej osobie. Rozpowszechnianie wizerunku bez podstawy prawnej może skutkować roszczeniami cywilnymi z tytułu naruszenia dóbr osobistych. Każdy człowiek powinien mieć możliwość tworzenia własnej tożsamości i wizerunku, także w środowisku cyfrowym, do decydowania o tym, co chce publikować na swój temat, a co powinno zostać w sferze prywatności.
2) Wizerunek dzieci podlega szczególnej ochronie, a ich interes oraz prawa i wolności mają charakter nadrzędny. Placówka dba o dobro dzieci i ich prywatność poprzez ostrożność przy publikowaniu zdjęć oraz uświadamianie zagrożeń związanych z nadmiernym rozpowszechnianiem wizerunku (hejt, kpiny, cyberprzemoc, przestępstwa na tle seksualnym, kradzież tożsamości).
3) Wykorzystanie wizerunku w placówce polega na utrwalaniu, wykorzystywaniu, rozpowszechnianiu, udostępnianiu, przechowywaniu oraz usuwaniu wizerunku osób - w szczególności:
   a) uczniów,
   b) rodziców, członków rodzin,
   c) gości, uczestników wydarzeń,
   d) pracowników, praktykantów, stażystów, wolontariuszy.
4) Zakres obejmuje w szczególności (katalog otwarty):
   a) fotografie, nagrania wideo, relacje „na żywo", materiały promocyjne, wywiady,
   b) publikacje w Internecie: strona internetowa, BIP, media społecznościowe, kanały wideo, chmury współdzielone,
   c) publikacje drukowane i fizyczne nośniki: kronika, gazetki, plakaty, ulotki, foldery, gabloty, tablice, tablo, zdjęcia klasowe, wystawy prac,
   d) materiały z wydarzeń: konkursy, wycieczki, zawody, uroczystości, zebrania.
5) Wykorzystanie wizerunku wymaga każdorazowo ustalenia właściwej podstawy prawnej:
   a) art. 6 ust. 1 lit. e RODO zadanie realizowane w interesie publicznym - np. działania dydaktyczno-wychowawcze realizowane w formie motywacyjnej. Przy czym gdyby rodzice uznali, że wpływa to negatywnie na dobro dziecka mogą wnieść sprzeciw z przyczyn związanych ze szczególną sytuacją,
   b) zgoda danej osoby lub rodzica (w przypadku dzieci) (załącznik nr 8A) - w szczególności przy publikacji zdjęć w Internecie:
      - zgoda musi być zrozumiała oraz określać kanały, cel, okres i zakres,
      - zgody nie łączy się z innymi oświadczeniami,
      - wycofanie zgody powinno być równie łatwe jak jej udzielenie,
   c) art. 81 ustawy o prawie autorskim i prawach pokrewnych - zezwolenia nie wymaga rozpowszechnianie wizerunku:
      - osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych,
      - osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza,
   d) każdy dodatkowy szczegół - np. imię, nazwisko, klasa czy wiek to osobna kategoria danych osobowych, a ich publikacja wymaga analogicznego uzasadnienia.

6) Zasady ogólne:
   a) odmowa zgody na publikację nie może wiązać się z żadnymi negatywnymi konsekwencjami (np. wykluczenie z aktywności),
   b) zakaz publikowania materiałów mogących naruszać godność, prywatność lub bezpieczeństwo ucznia (sytuacje emocjonalne, dyscyplinujące, wstydliwe, konfliktowe, ośmieszające oraz krępujące np. w niepełnym ubraniu, w trakcie czynności higienicznych, czy wizyty w gabinecie specjalistycznym),
   c) zakaz publikowania wraz z wizerunkiem informacji umożliwiających profilowanie (np. adres, harmonogram pobytu, szczegóły zdrowotne, dane o sytuacji rodzinnej),
   d) weryfikacja tła (tablice z danymi, listy, dokumenty).
7) Dobre praktyki i rozwiązania ograniczające ryzyko (szczególnie w Internecie):
   a) preferowanie ujęć grupowych i sytuacyjnych,
   b) ograniczenie łączenia wizerunku z innymi danymi: imieniem i nazwiskiem, klasą czy wiekiem. Jeżeli jest to uzasadnione i objęte zgodą należy kierować się zasadą minimalizacji (np. imię + klasa, imię + laureat konkursu, uczeń + klasa),
   c) usunięcie metadanych przed publikacją w sieci (np. informacji o geolokalizacji),
   d) ograniczenie czasu dostępności publikacji (np. usunięcie po zakończeniu roku szkolnego, etapu edukacyjnego lub po określonym terminie),
   e) pytanie ucznia o zgodę na zrobienie i publikację zdjęcia/nagrania. Zgoda rodzica nie jest równoznaczna ze zgodą ucznia,
   f) uszanowanie zdania ucznia, jeśli nie chce znaleźć się na zdjęciu lub nagraniu.
8) Podstawy dopuszczalności wykorzystania wizerunku i danych osobowych:
   a) bez zgody:

   Art. 81 ustawy o prawie autorskim i prawach pokrewnych:

   i. wizerunek osoby stanowiącej jedynie **szczegół całości** takiej jak zgromadzenie, krajobraz, publiczna impreza - spełniający następujące kryteria:
      - wizerunek jest jedynie elementem ujęcia, stanowi jego małą część, której usunięcie nie zmieniłoby przedmiotu i charakteru tego, co jest pokazane,
      - zdjęcie nie powinno być zdjęciem pozowanym (pozowanie niejako oznaczałoby, że dana osoba jest jednak istotnym elementem zdjęcia),
      - zdjęcie z określonego wydarzenia (np. uroczystości, wycieczki, imprezy, pikniku czy warsztatów) ma na celu przedstawienie danego wydarzenia, a jego uczestnicy nie będą elementem dominującym ujęcia, fotografia zostanie wykonana bez zbliżeń na daną postać czy małą grupę osób.

      Przykłady: panorama sali na akademii, ujęcie z tyłu na apelu, krajobrazowe ujęcie na wycieczce (daleki plan), szerokie ujęcie (twarze są małe i nieczytelne), dekoracje i scenografia - osoby są przypadkowym tłem wydarzenia,

   ii. wizerunek osoby powszechnie znanej w związku z pełnieniem przez nią funkcji publicznych,

   Art. 6 ust. 1 lit. e RODO zadanie realizowane w interesie publicznym:

   iii. **w przestrzeni wewnętrznej** placówki, w celach dydaktyczno-wychowawczych:

- umieszczanie danych uczniów w specjalnych strefach - ma na celu ich wyróżnienie za szczególne osiągnięcia. Taka praktyka stanowi element działań wychowawczych, nagradzających wysiłek włożony w realizację powierzonych zadań. Przyczynia się też do wzmocnienia poczucia własnej wartości,
- ogłaszanie osiągnięć edukacyjnych uczniów w placówce - ma charakter motywacyjny i promuje pozytywne wzorce zachowań,
- umieszczanie pod różnego rodzaju pracami podpisów zawierających imię, nazwisko i klasę - kształtuje postawy doceniania wysiłku i pracy własnej,
- umieszczanie materiałów z życia placówki - tworzy pozytywny klimat, buduje wspólnotę i historię placówki,
- imię, nazwisko czy klasa w społeczności placówki nie są danymi anonimowymi. Ich udostępnianie w relacjach międzyludzkich wewnątrz placówki zapewnia nawiązywanie normalnych relacji międzyludzkich.

Przykłady: zdjęcie z uroczystości wręczenia nagród na tablicy osiągnięć, przedstawienie osiągnięć konkretnego ucznia na apelu, wizerunek w kronice placówki, prowadzenie tablo, zdjęcie klasowe, wyczytywanie imion i nazwisk przy sprawdzaniu obecności, podpisane szafki,

iv. zdjęcie w legitymacji,

b) wymagana zgoda:

i. co do zasady publikacja wizerunku i danych osobowych **w Internecie** wymaga zgody:

- jeśli wizerunek osoby można rozpoznać, a materiał ma trafić do Internetu - stosuje się zgodę, nawet gdy teoretycznie można dyskutować o „szczególe całości",

Przykłady: post w mediach społecznościowych (osoby są rozpoznawalne), umieszczenie na stronie internetowej zdjęcia klasowego/grupowego, publikacja danych osobowych laureata konkursu, film z wizerunkiem uczniów na YouTube, transmisja online wydarzenia, newsletter publiczny,

ii. materiały promocyjne na zewnątrz:

- materiały dla gości,
- zdjęcie w miejscu ogólnodostępnym (korytarz przy wejściu, poczekalnia),

iii. przechowywanie dokumentów aplikacyjnych celem wykorzystania ich w przyszłych rekrutacjach,

iv. przetwarzanie danych osobowych osób aplikujących na wolne stanowisko, innych niż te wynikające z art. 22^1 § 1 Kodeksu pracy,

v. przetwarzanie danych osobowych pracowników, innych niż te zawarte w art. 22^1§ 1 i 3 Kodeksu pracy.

9) W przypadku wycofania zgody:

a) placówka niezwłocznie blokuje dalsze wykorzystanie wizerunku i dokonuje przeglądu publikacji oraz usuwa/anonimizuje materiały, o ile brak innej podstawy prawnej dalszego przetwarzania,

b) jeżeli placówka upubliczniła dane osobowe, to podejmuje rozsądne działania, by poinformować innych administratorów przetwarzających kopie/odnośniki, by je usunęli,

c) gdy placówka przetwarza bardzo dużą liczbę materiałów zawierających wizerunek, może poprosić o doprecyzowanie, których informacji lub czynności przetwarzania dotyczy żądanie - w szczególności poprzez wskazanie przybliżonego okresu publikacji, wydarzenia, opisu ujęcia lub linków. Prośba o doprecyzowanie służy wyłącznie usprawnieniu realizacji żądania i nie wstrzymuje działań placówki w zakresie, w jakim placówka jest w stanie zidentyfikować publikacje na podstawie posiadanych informacji,

d) w przypadku materiałów drukowanych - zaprzestaje dalszej dystrybucji. Wobec materiałów już rozpowszechnionych podejmuje racjonalne działania ograniczające.

10) Okres wykorzystania materiałów:

a) dopuszczalne jest wykorzystanie wizerunku tak długo, jak jest to konieczne do osiągnięcie celu i istnieje podstawa prawna,

b) wizerunek uczniów opuszczających placówkę nie będzie już publikowany bez ponownej zgody,

c) retencję ustala się zgodnie z zasadą ograniczenia przechowywania oraz z uwzględnieniem przepisów kancelaryjno-archiwalnych (JRWA).

11) W przypadku organizowania sesji fotograficznych z profesjonalnym fotografem rozróżnia się dwa modele współpracy:

a) na zasadzie bezpośredniej umowy między fotografem a rodzicami - w takim wypadku to fotograf jest administratorem danych i ponosi pełną odpowiedzialność za przetwarzanie danych osobowych. Placówka pełni rolę wspierającą:

- udostępnia wyznaczoną strefę w określonym czasie,
- odpowiada za bezpieczeństwo organizacyjne i fizyczne,
- zapewnia alternatywę dla uczniów nieuczestniczących w sesji,
- nie przekazuje fotografowi danych osobowych (list uczniów i danych kontaktowych),

b) fotograf działa na zlecenie placówki - jeśli to placówka zatrudnia fotografa wymagane jest zawarcie umowy powierzenia. Placówka:

- ustala cele i zasady przetwarzania danych,
- wydaje instrukcje dla fotografa,
- odpowiada za realizację obowiązku informacyjnego i posiadanie podstawy prawnej (zgód).

12) Utrwalanie wizerunku przez osoby postronne:

a) rodzice (i osoby bliskie) rejestrujące wizerunek podczas wydarzeń w placówce:

- dopuszcza się wykonywanie zdjęć/nagrań przez rodziców wyłącznie na użytek prywatny i w zakresie obejmującym własne dziecko,
- rodzic nie jest uprawniony do utrwalania wizerunku innych uczniów w sposób pozwalający na ich identyfikację, w szczególności pojedynczego ucznia lub małej grupy niebędącej jego rodziną,
- placówka informuje przed wydarzeniem (ustnie lub przy wejściu), że osoby prywatne utrwalają wizerunek na własny użytek, a publikacja wizerunku innych uczniów może naruszać ich prawa (załącznik nr 8B),
- placówka może wyznaczyć strefę fotografowania i ramy czasowe (np. 2-3 minuty na zdjęcia na początku i na końcu),
- w razie naruszenia zasad organizator ma prawo przerwać rejestrowanie wizerunku i wezwać do usunięcia materiału.

b) dziennikarze, fotoreporterzy jako odrębni administratorzy danych:
   - w placówce obowiązuje reguła, że fotografowanie/nagrywanie jest możliwe wyłącznie za zgodą dyrektora lub osoby przez niego upoważnionej,
   - podmioty utrwalające wizerunek zobowiązane są do przestrzegania zasad obowiązujących w placówce,
   - w przypadku naruszenia zasad, dyrektor ma prawo przerwać realizację materiału i wezwać media do opuszczenia terenu.

11. Wydarzenia międzyszkolne

1) Odpowiedzialność za właściwe przetwarzanie danych osobowych ciąży na organizatorze wydarzenia (konkursu, zawodów lub olimpiady).
2) Przy organizacji tego typu wydarzeń konieczne jest pozyskanie zgody na przetwarzanie danych osobowych, które musi się odnosić do każdego rodzaju operacji przetwarzania, w tym do rozpowszechniania wizerunku (załącznik nr 9A/B). Taką zgodę wyraża rodzic lub dana osoba w przypadku osoby pełnoletniej. Ani dyrektor, ani nauczyciel nie jest upoważniony do wyrażenia takiej zgody w imieniu ucznia.

12. Gabinet pielęgniarki/higienistki

1) Gabinet profilaktyki zdrowotnej obejmuje uczniów podstawową opieką zdrowotną. Jej realizacja odbywa się na podstawie porozumienia zawartego pomiędzy podmiotem leczniczym i placówką oraz umowy o udzielanie świadczeń opieki zdrowotnej zawartej między podmiotem leczniczym i Narodowym Funduszem Zdrowia.
2) Dyrektor placówki na podstawie art. 68 ust. 1 pkt 11 ustawy Prawo oświatowe udostępnia pielęgniarce szkolnej imię, nazwisko i numer PESEL ucznia celem właściwej realizacji profilaktycznej opieki zdrowotnej nad dziećmi i młodzieżą.
3) Pielęgniarka lub higienistka nie jest pracownikiem placówki oraz nie jest podległa służbowo dyrektorowi. Na dyrektorze ciąży obowiązek zapewnienia uczniom dostępu do gabinetu profilaktyki zdrowotnej tj. zawarcie umowy i zapewnienie miejsca. Poza kompetencją dyrektora są natomiast kwestie samego świadczenia podstawowej opieki zdrowotnej, jak i zasady postępowania z dokumentacją tworzoną w wyniku jej świadczenia. Obowiązek właściwego przechowywania dokumentacji medycznej ciąży na podmiocie leczniczym świadczącym opiekę zdrowotną

13. Udzielanie informacji przez telefon

1) Przy udzielaniu informacji przez telefon najważniejsze jest zidentyfikowanie dzwoniącego oraz ustalenie, czy jest on uprawniony do pozyskania informacji o uczniu. Dlatego w takich sytuacjach ważne jest dążenie do potwierdzenie, że osoba dzwoniąca jest tą, za którą się podaje. Informacjami służącymi do weryfikacji dzwoniącego może być np. imię, nazwisko i wiek ucznia, imiona rodziców, w co jest ubrany, w której jest klasie, nazwisko wychowawcy itp.
2) W przypadku wątpliwości co do tożsamości osoby usiłującej pozyskać informacje dotyczące ucznia, powinno się odmówić ich udzielenia, ewentualnie podać informacje ogólne bez konkretnych danych.
3) W przypadku sytuacji nagłych placówka kontaktuje się z rodzicem, aby móc przekazać lub pozyskać niezbędne informacje. Dzięki temu nie powinno dochodzić do sytuacji, w której odmawia się rodzicom udzielenia informacji o nagłym zdarzeniu czy zaistniałym niebezpieczeństwie dotyczącym ucznia.
4) W sytuacjach kryzysowych zazwyczaj nie ma potrzeby udzielania szczegółowych informacji o stanie zdrowia. Wystarczającymi informacjami przekazywanymi przez telefon może być np. wskazanie, gdzie obecnie znajduje się uczeń, miejsce zdarzenia, rodzaj zdarzenia. Konieczna jest jednak ostrożność, komu udziela się takich informacji.

5) Podczas rozmowy telefonicznej należy upewnić się, że w bliskim otoczeniu nie ma nieupoważnionych osób, które mogłyby usłyszeć informacje podlegające ochronie.

14. Dokumentacja związana z zatrudnieniem

1) Dokumentacja pracownicza jest prowadzona i przechowywana zgodnie z rozporządzeniem w sprawie dokumentacji pracowniczej.
2) Dokumenty rekrutacyjne przyjmuje się wyłącznie kanałami zatwierdzonymi przez placówkę (osobiście/poczta/e-Doręczenia/służbowa poczta elektroniczna /platforma rekrutacyjna). Zakres danych w rekrutacji ogranicza się do danych wymaganych przepisami tj. imię, nazwisko, data urodzenia, dane kontaktowe, wykształcenie, kwalifikacje zawodowe, przebieg dotychczasowego zatrudnienia. Dane dodatkowe są przyjmowane tylko, gdy ich przekazanie nastąpiło z inicjatywy kandydata.
3) Akta osobowe prowadzi się oddzielnie dla każdego pracownika, zgodnie z obowiązującą strukturą części akt określoną w przepisach wykonawczych. Dokumenty zawierające dane szczególnej kategorii (np. dane o zdrowiu) są w aktach przechowywane wyłącznie wtedy, gdy wynika to z przepisów.
4) Placówka przetwarza w obszarze medycyny pracy wyłącznie dane niezbędne do wykonania obowiązków pracodawcy, tj. skierowania na badania profilaktyczne, orzeczenia lekarskie o braku przeciwwskazań lub przeciwwskazaniach do pracy na określonym stanowisku, terminy ważności badań. Placówka nie żąda i nie przechowuje wyników badań, historii choroby ani innej szczegółowej dokumentacji medycznej (informacje te pozostają w podmiocie medycyny pracy). Skierowania i orzeczenia przechowuje się w aktach osobowych.
5) W ramach Zakładowego Funduszu Świadczeń Socjalnych:
   a) dane osobowe są pozyskiwane i wykorzystywane wyłącznie w celu:
      - przyznania ulgowych usług, świadczeń i dopłat,
      - ustalenia wysokości świadczenia,
      - ewentualnego dochodzenia praw lub roszczeń związanych z przyznaniem świadczeń,
   b) podstawową formą przekazania danych przez osobę uprawnioną jest oświadczenie. Pracodawca może żądać udokumentowania danych osobowych wyłącznie w zakresie niezbędnym do ich potwierdzenia poprzez:
      - wgląd w dokument przedstawiony przez osobę uprawnioną i sporządzenie adnotacji służbowej w aktach sprawy (datę weryfikacji, wskazanie rodzaju dokumentu, zakres danych, podpis osoby weryfikującej, numer sprawy),
      - dołączenie kopii/odpisu dokumentu do dokumentacji ZFŚS - wyłącznie pod warunkiem, że:

        - jest to niezbędne do udokumentowania przesłanek przyznania świadczenia i jego wysokości (zgodnie z Regulaminem), a nie da się tego osiągnąć za pomocą samej adnotacji,

        - kopia obejmuje wyłącznie fragment niezbędny do potwierdzenia danych, a pozostałe dane (jeśli występują) są zanonimizowane (fizycznie zakrywane przed wykonaniem kopii albo zaczerniane na kopii),
   c) zakazuje się gromadzenia informacji nadmiarowych, w szczególności przyczyn zgonu i szczegółowych danych medycznych,
   d) placówka przetwarza dane osobowe przez okres niezbędny do przyznania świadczenia oraz przez okres niezbędny do dochodzenia praw lub roszczeń,
   e) dane osobowe podlegają przeglądowi co najmniej raz w roku i usunięciu, gdy są zbędne,

f) dokumentację ZFŚS przechowuje się oddzielnie od akt osobowych.

---

§ 5.

Środki bezpieczeństwa

1. Postanowienia ogólne

1) Placówka zapewnienia bezpieczeństwo zasobów informacyjnych i technicznych, w tym zabezpieczenia pomieszczeń, sprzętu komputerowego i dokumentacji przed dostępem osób nieuprawnionych, zniszczeniem, kradzieżą lub uszkodzeniem.
2) Środki bezpieczeństwa stosowane są do wszystkich pomieszczeń, w których przetwarzane są informacje lub przechowywana jest dokumentacja, sprzęt komputerowy, nośniki danych i infrastruktura sieciowa.
3) Wszystkie zastosowane środki bezpieczeństwa zostały dobrane adekwatnie do ryzyka.

2. Zabezpieczenia fizyczne

1) Miejsca z dokumentacją lub sprzętem IT (np. serwerownia, szafy sieciowe, sekretariat, gabinet pedagoga, archiwum) są:
   a) zamykane na klucz,
   b) dostępne wyłącznie dla osób upoważnionych,
   c) objęte kontrolą dostępu (np. monitoring wizyjny, system kontroli dostępu na kod).
2) Dokumentacja jest przechowywana w zamykanych szafach i biurkach oraz dostępna wyłącznie dla upoważnionych pracowników. Dokumenty są umieszczane na półkach, regałach i w szufladach z dala od podłogi (zabezpieczenie przed zalaniem).
3) Obowiązują zasady opisane w § 3:
   a) czystego biurka,
   b) czystego ekranu,
   c) czystej drukarki,
   d) czystego kosza,
   e) czystej tablicy.
4) Goście (np. serwis, rodzice) mogą przebywać w jednostce wyłącznie pod opieką pracownika placówki.
5) Budynek jest zabezpieczany po godzinach pracy poprzez:
   a) zamykanie wszystkich pomieszczeń i okien,
   b) alarm,
   c) monitoring,
   d) nadzór (firma ochroniarska).
6) Klucze/karty dostępowe podlegają ewidencji. Zabronione jest ich przekazywanie osobom trzecim.
7) W pomieszczeniu serwerowym utrzymywane są odpowiednie warunki środowiskowe (temperatura, wilgotność) np. klimatyzacja.
8) Dla kluczowych urządzeń funkcjonuje zasilanie awaryjne (UPS) oraz stosowane jest zabezpieczenie przeciwprzepięciowe.
9) Budynki zostały wyposażone w gaśnice, oświetlenie awaryjne i system odgromowy.
10) Utrzymywanie drożnych dróg ewakuacyjnych.

3. Zabezpieczenia organizacyjne

1) Dostęp do informacji wyłącznie dla osób przeszkolonych z SZBI i zasad ochrony danych osobowych oraz posiadających stosowne upoważnienie.
2) Zobowiązanie do zachowania tajemnicy wszystkich osób mających dostęp do danych osobowych.
3) Nadawanie uprawnień w systemach informatycznych upoważnionym osobom.
4) Pracownicy placówki przetwarzający dane osobowe podlegają obowiązkowym okresowym szkoleniom z zakresu ochrony danych. Szkolenie wstępne odbywa się przed dopuszczeniem pracownika do pracy z danymi.
5) Podpisywanie umów powierzenia przetwarzania danych z podmiotami zewnętrznymi.
6) Stosowanie anonimizacji i pseudonimizacji.
7) Placówka prowadzi rejestr incydentów i naruszeń oraz dokumentuje wszelkie stwierdzone niezgodności. Każdy incydent podlega analizie przyczyn i skutków, a następnie wdrażane są działania korygujące zapobiegające powtórzeniu się podobnej sytuacji.
8) Stały monitoring zgodności przetwarzania z prawem oraz niniejszym SZBI poprzez okresowe audyty wybranych obszarów przetwarzania danych.
9) Co najmniej raz w roku dokonywany jest przegląd SZBI w celu oceny skuteczności stosowanych zabezpieczeń, aktualności dokumentacji oraz zidentyfikowania ewentualnych nowych ryzyk lub potrzeb w zakresie ochrony danych.

4. Zabezpieczenia techniczne

1) Placówka korzysta wyłącznie z legalnego oprogramowania, które jest na bieżąco aktualizowane. Automatyczne aktualizacje systemu operacyjnego oraz kluczowego oprogramowania są włączone.
2) Zakaz instalowania nieautoryzowanego oprogramowania na służbowych urządzeniach, otwierania plików niewiadomego pochodzenia oraz podłączania prywatnych nośników danych bez zgody dyrektora lub ASI.
3) Urządzenia służbowe posiadają aktualne oprogramowanie antywirusowe z włączoną funkcją automatycznego skanowania i monitorowania w czasie rzeczywistym.
4) Zabezpieczenie systemów informatycznych przed dostępem z sieci publicznej (Internet) przy pomocy odpowiednio skonfigurowanej zapory sieciowej (firewall).
5) Zabezpieczenie urządzeń IT przed nieautoryzowanym dostępem poprzez indywidualne identyfikatory użytkowników i silne hasła dostępowe.
6) Stosowanie mechanizmów uwierzytelnienia zwiększających bezpieczeństwo systemów, np. wieloetapowa weryfikacja (2FA, MFA), jeżeli takie funkcje są dostępne.
7) Automatyczna blokada ekranu w przypadku braku aktywności przez zdefiniowany okres czasu.
8) Nośniki danych i urządzenia przenośne są szyfrowane. Szyfrowanie stosuje się także przy przesyłaniu informacji poufnych.
9) Regularne archiwizowanie i tworzenie kopii zapasowych baz danych.
10) Systemy informatyczne, o ile to możliwe, są skonfigurowane tak, aby rejestrować istotne zdarzenia (logi).
11) W przypadku korzystania z usług chmurowych dostawcy tych usług gwarantują odpowiedni poziom ochrony danych (posiadają certyfikaty lub spełniają standardy bezpieczeństwa, a zakres powierzonych danych jest ograniczony do niezbędnego minimum).
12) Placówka stosuje system monitoringu wizyjnego.

13) Niszczenie dokumentów i nośników elektronicznych odbywa się w sposób uniemożliwiający odtworzenie.

14) Drukarki i urządzenia wielofunkcyjne umieszczone są w strefie nadzorowanej i nie przechowują dokumentów po wydruku (automatyczne czyszczenie buforu).

15) Okablowanie sieciowe i gniazda sieci w miejscach ogólnodostępnych są zabezpieczone przed nieautoryzowanym podłączeniem.

16) Urządzenia informatyczne posiadają wydzieloną sieć energetyczną. Gniazda elektryczne tej sieci zabezpieczone są przed podłączeniem innego urządzenia poprzez zastosowanie gniazd z blokadą.

5. Obsługa osób postronnych

1) Wejście osób trzecich do placówki odbywa się:
   a) wyłącznie przez wyznaczone wejście główne,
   b) po zgłoszeniu celu wizyty pracownikowi placówki,
   c) pod nadzorem pracownika placówki.
2) Placówka nie kopiuje dokumentów tożsamości oraz nie żąda numeru PESEL od wchodzących.

6. Zarządzanie kluczami i kartami dostępu

1) W placówce prowadzona jest ewidencja wszystkich fizycznych lub elektronicznych nośników umożliwiających dostęp do pomieszczeń.
2) Ewidencja kluczy/kart (załącznik nr 11) jest zabezpieczona przed dostępem osób trzecich.
3) Klucze zapasowe przechowywane są w zamknięciu i wykorzystywane w wyjątkowych sytuacjach.
4) Dostęp do pomieszczeń przyznawany jest przez dyrektora na podstawie zakresu obowiązków i zgodnie z zasadą minimalnego dostępu.
5) Klucze do pomieszczeń wydawane i zdawane są w pokojach nauczycielskich, portierniach, sekretariacie i w pomieszczeniu kierownika gospodarczego. Pobrane klucze pozostają pod osobistym nadzorem osób upoważnionych.
6) Zabrania się:
   a) dorabiania kluczy bez zgody dyrektora,
   b) przekazywania kluczy/kart osobom trzecim.
7) Utrata klucza/karty jest niezwłocznie zgłaszana dyrektorowi, który ocenia ryzyko i decyduje o wymianie zamka lub dezaktywacji karty. W przypadku ryzyka dostępu do danych wymagana jest konsultacja z IOD.
8) Placówka nie wykorzystuje danych biometrycznych w celu kontroli dostępu.
9) Klucze służące do zabezpieczenia biurek i szaf w godzinach pracy pozostają pod nadzorem pracowników, którzy ponoszą odpowiedzialność za ich należyte zabezpieczenie. Po zakończeniu pracy klucze muszą być przechowywane w zabezpieczonym miejscu.
10) W przypadku zakończenia umowy wszystkie klucze i karty zwracane są najpóźniej w ostatnim dniu współpracy.

---

§ 6.

Bezpieczeństwo zasobów informatycznych

1. Zapobieganie i wykrywanie złośliwego oprogramowania

1) Placówka w celu realizacji swoich zadań wykorzystuje sprzęt IT, w tym
   a) komputery, urządzenia mobilne, nośniki danych,
   b) drukarki, urządzenia wielofunkcyjne,
   c) urządzenia sieciowe.
2) Urządzenia służbowe mogą być wykorzystywane wyłączenie w celach służbowych i są zabezpieczone przed dostępem osób nieuprawnionych.
3) Na urządzeniach instalowane jest jedynie legalne oprogramowanie, które jest niezbędne do realizacji zadań i zostało zatwierdzone przez dyrektora lub ASI.
4) Wszystkie systemy są regularnie aktualizowane. Aktualizacje krytyczne instaluje się niezwłocznie po ich wydaniu lub zgodnie z zaleceniami producenta.
5) Systemy informatyczne chronione są przed działaniem wirusów i złośliwego oprogramowania za pomocą odpowiednio skonfigurowanego systemu antywirusowego oraz zapory sieciowej (firewall). Definicje służące do rozpoznawania nowych zagrożeń są wprowadzane w systemie niezwłocznie po ich opublikowaniu przez producenta. Dane i nośniki wymienne sprawdzane są automatycznie w czasie rzeczywistym.
6) Okablowanie sieciowe i gniazda sieci w miejscach ogólnodostępnych są zabezpieczone przed nieautoryzowanym podłączeniem.
7) W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:
   a) podejmowania prób przełamania lub ominięcia stosowanych zabezpieczeń,
   b) odwiedzania stron internetowych niezwiązanych z pełnionymi obowiązkami służbowymi, a w szczególności stron nienależących do wiarygodnych organizacji lub podmiotów, co może prowadzić do pobrania złośliwego oprogramowania i nieuprawnionego dostępu do systemu informatycznego,
   c) pobierania nielegalnych plików lub treści niezgodnych z misją placówki,
   d) samodzielnego przeprowadzania jakichkolwiek zmian oprogramowania i jego konfiguracji, które miałyby wpływ na bezpieczeństwo systemu informatycznego.
8) W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik jest zobowiązany powiadomić dyrektora lub ASI. Niepokojące objawy to:
   a) istotne spowolnienie działania całego systemu informatycznego,
   b) nietypowe działanie systemu i aplikacji,
   c) nietypowe komunikaty, błędy,
   d) nagła utrata danych lub nietypowe zmiany w danych,
   e) wystąpienie w krótkim czasie dużej liczby nieudanych prób logowania,
   f) pojawienie się nowych nieautoryzowanych kont użytkowników.
9) Użytkownicy zobowiązani są do bieżącego zgłaszania awarii, utraty i kradzieży sprzętu dyrektorowi lub ASI. W przypadku utraty lub kradzieży podejmowana jest próba zdalnego usunięcia danych.
10) Obowiązuje podział sieci Wi-Fi na:
   a) sieć administracyjną (dla uprawnionych pracowników, zabezpieczona co najmniej WPA2-PSK),
   b) sieć uczniowską (z ograniczeniami),
   c) sieć gościnną (bez dostępu do zasobów placówki).

11) Za konfigurację i utrzymanie sieci odpowiada ASI, w tym:
   a) w miarę możliwości technicznych - włączenie logowania zdarzeń (logi systemowe, logi dostępu) oraz okresowe przeglądy logów pod kątem anomalii. Informacje w dziennikach systemów przechowywane są przez okres co najmniej 24 miesięcy, o ile przepisy szczególne nie wymagają dłuższego okresu,
   b) dostęp administracyjny mają tylko upoważnione osoby, a logowanie odbywa się z sieci lokalnej lub zdalnie z użyciem szyfrowanego połączenia (VPN, SSH),
   c) na komputerach blokuje się nieużywane porty i usługi (np. wyłączenie zbędnych usług systemowych, blokada bootowania z USB, aby utrudnić uruchomienie niepożądanych systemów),
   d) kluczowe urządzenia sieciowe (np. router) są objęte harmonogramem regularnych przeglądów oraz aktualizacji firmware,
   e) zmiana fabrycznych haseł dostępowych do interfejsów zarządzania urządzeniami (np. routery Wi-Fi),
   f) okresowy przeglądy infrastruktury technicznej.

2. Zarządzanie zasobami

1) Sprzęt komputerowy, urządzenia mobilne, nośniki danych i inne urządzenia techniczne przekazywane użytkownikom do użytku służbowego są nadzorowane i ewidencjonowane.
2) Sprzęt wydaje się na podstawie decyzji dyrektora i dokumentuje się Protokołem przekazania sprzętu (załącznik nr 12A). Użytkownik staje się odpowiedzialny za powierzone urządzenie i dba o jego bezpieczeństwo (m.in. hasła i aktualizacje).
3) Zwrot sprzętu następuje:
   a) w dniu zakończenia zatrudnienia lub współpracy,
   b) na żądanie dyrektora,
   c) w przypadku wymiany sprzętu na inny.
4) Zwrot sprzętu dokumentuje się Protokołem zwrotu sprzętu (załącznik nr 12B).
5) ASI lub osoba wyznaczona:
   a) przygotowuje sprzęt (konfiguracja, oprogramowanie, zabezpieczenia, oznakowanie),
   b) informuje użytkownika o zasadach korzystania,
   c) dokonuje okresowego przeglądu urządzeń,
   d) po zwrocie urządzenia weryfikuje jego stan techniczny i usuwa dane,
   e) prowadzi elektroniczny Rejestr zasobów IT (załącznik nr 12C/D) i dokonuje jego aktualizacji przy wydaniu, zwrocie lub likwidacji zasobu.
6) W przypadku wynoszenia sprzętu poza budynek placówki urządzenie musi zostać odpowiednio zabezpieczone na czas transportu.
7) Naprawa lub konserwacja sprzętu może być zlecona serwisowi gwarantującemu bezpieczeństwo informacji. Przed oddaniem sprzętu do naprawy - o ile to możliwe - usuwane są informacje lub nośnik danych. Gdy naprawa dotyczy nośnika danych podpisuje się umowę powierzenia lub klauzulę o zachowaniu poufności.
8) Sprzęt wycofywany z użycia jest pozbawiany danych i przekazywany do utylizacji zgodnie z obowiązującymi przepisami.

3. Nadawanie, zmiana i odbieranie dostępu

1) Uprawnienia do systemów i zasobów informatycznych nadawane są wyłącznie osobom posiadającym upoważnienie. Przydzielany poziom dostępu jest zgodny z zakresem obowiązków oraz zasadą najmniejszych uprawnień.
2) Każdy użytkownik posiada indywidualne konto w celu zapewnienia kontroli nad dostępem do danych osobowych i zasobów informacyjnych. Zakazane jest współdzielenie kont lub ich udostępnianie.
3) Konta administratora systemu używane są wyłącznie w uzasadnionych przypadkach i podlegają szczególnej kontroli.
4) Użytkownik zobowiązany jest do:
   a) korzystania z przyznanych uprawnień zgodnie z przeznaczeniem,
   b) ochrony danych logowania,
   c) zgłaszania nieprawidłowości w działaniu systemów do dyrektora lub ASI.
5) Wszelkie logowania i próby logowania są rejestrowane.
6) Zmiana uprawnień następuje przy zmianie stanowiska, zakresu zadań lub stwierdzeniu nieprawidłowości.
7) Uprawnienia odbiera się niezwłocznie w przypadku:
   a) rozwiązania umowy o pracę lub innej formy współpracy - najpóźniej w dniu rozwiązania stosunku prawnego następuje blokada lub usunięcie wszystkich kont tego użytkownika w systemach (np. login do sieci, e-mail, dostęp do platform),
   b) ustania potrzeby posiadania dostępu,
   c) naruszenia zasad bezpieczeństwa.
8) Uprawnienia są przeglądane nie rzadziej niż raz na 12 miesięcy.

4. Hasła i uwierzytelnianie

1) Zasady stosowania haseł oraz metod uwierzytelniania mają zapewnić bezpieczeństwo wszystkich systemów informatycznych:
   a) oprogramowania, kont e-mail, aplikacji i platform internetowych,
   b) urządzeń mobilnych i komputerów,
   c) systemu monitoringu, serwerów i urządzeń sieciowych.
2) Każdy użytkownik posiada indywidualne konto i hasło.
3) Hasło musi spełniać następujące wymagania:
   a) składać się z co najmniej 10 znaków, rekomendowana długość to 12 znaków,
   b) zawierać cztery grupy znaków :
      - wielką literę (A-Z),
      - małą literę (a-z),
      - cyfrę (0-9),
      - znak specjalny (!@#$%^&*()_+=-{},.;/?),
   c) nie może zawierać:
      - imienia, nazwiska użytkownika,
      - nazwy placówki,
      - prostych sekwencji (np. „123", „abcd", „qwerty"),
   d) nie może być ponownie używane przez minimum 6 cykli zmian.
4) Użytkownicy zobowiązani są do zmiany hasła:
   a) przy pierwszym logowaniu,

b) po resecie hasła przez ASI,

c) w razie podejrzenia, że hasło mogło zostać ujawnione lub złamane,

d) co najmniej raz na 90 dni.

5) Jeżeli dany system na to pozwala, zaleca się włączenie uwierzytelniania wieloskładnikowego (MFA, 2FA), które wymaga podania hasła oraz dodatkowego elementu (np. kod SMS, kod z aplikacji uwierzytelniającej, potwierdzenie w aplikacji mobilnej). Konta administracyjne oraz konta z dostępem do danych wrażliwych obowiązkowo wymagają stosowania uwierzytelniania wieloskładnikowego.

6) Użytkownicy są zobowiązani chronić poufność swoich haseł przed innymi osobami:

a) zabronione jest:

- udostępnianie haseł (nigdy, w żadnej sytuacji nie należy ujawniać hasła),
- zapisywanie haseł w miejscach dostępnych dla osób postronnych (na kartkach, biurku, monitorze, w notesach, zeszytach, kalendarzach),
- zapisywanie haseł w plikach nieszyfrowanych lub w przeglądarce,
- wprowadzanie haseł w sposób widoczny dla osób trzecich,

b) hasła powinny:

- być przechowywane w sposób zaszyfrowany (np. w menedżerze haseł),
- różnić się od haseł używanych w celach prywatnych.

7) Systemy powinny automatycznie blokować dostęp w przypadku kilku nieudanych prób logowania (wg ustawień danego oprogramowania np. trzykrotne wprowadzenie błędnego hasła blokuje konto na okres 30 minut).

8) Urządzenia przed odejściem od stanowiska należy zablokować (np. skrót klawiszowy Windows+L), co wymusza konieczność ponownego wpisania hasła w celu odblokowania.

9) Urządzenia są automatycznie blokowane w przypadku braku aktywności przez maksymalnie 10 minut.

10) Hasła do kont uprzywilejowanych (administratorów, kluczowych urządzeń sieciowych) przechowywane są w sposób szczególnie zabezpieczony - np. w menedżerze haseł z lokalnym szyfrowaniem danych lub w zapieczętowanej kopercie pod zamknięciem (na wypadek sytuacji awaryjnej). Dostęp do tych informacji jest ściśle ograniczony.

5. Nośniki i szyfrowanie danych

1) Szyfrowanie pozwala na zabezpieczenie danych przed dostępem niepowołanych osób poprzez zakodowanie:

a) nośników przenośnych (pendrive, dysk zewnętrzny, CD/DVD),

b) urządzeń mobilnych używanych poza placówką (laptopy, tablety),

c) informacji poufnych,

d) kopii zapasowych.

2) Szyfrowanie odbywa się za pomocą narzędzi wykorzystujących algorytm uznawany za bezpieczny (m.in. AES-256) np. BitLocker (Windows), FileVault (macOS), LUKS (Linux), VeraCrypt, 7-Zip.

3) Hasło/klucz nie może być przechowywane razem z urządzeniem lub plikami.

4) Hasło przekazuje się innym kanałem niż plik (np. e-mail + telefon).

5) Dozwolone jest używanie wyłącznie nośników zatwierdzonych przez dyrektora lub ASI. Przed użyciem nośnik musi zostać przeskanowany oprogramowaniem antywirusowym.

6) Nośniki muszą być przechowywane w miejscu zabezpieczonym fizycznie.
7) W przypadku korzystania z usług zdalnych placówka wybiera dostawców zapewniających szyfrowanie danych w transmisji (HTTPS/TLS).

6. Kopie zapasowe

1) Tworzenie kopii zapasowych zapewnia możliwość odtworzenia kluczowych danych i systemów w przypadku ich utraty lub uszkodzenia, w tym danych osobowych, dokumentów księgowo-kadrowych, plików dydaktycznych, dziennika elektronicznego, poczty e-mail oraz systemów wspierających funkcjonowanie placówki.
2) Kopie tworzy się:
   a) codziennie - dla danych krytycznych,
   b) co tydzień - dla danych pomocniczych,
   c) co miesiąc - archiwalne,
   d) automatycznie - jeśli system na to pozwala,
   e) ręcznie - w pozostałych przypadkach.
3) W przypadku usług dostarczanych zdalnie, kopia zapasowa może być realizowana przez dostawcę usługi, jeżeli zapewnia taką możliwość np. System Informacji Oświatowej, dziennik elektroniczny, chmura internetowa.
4) Kopie zapasowe przechowuje się:
   a) na nośnikach lokalnych z ograniczonym dostępem (serwer backupowy),
   b) na zabezpieczonych nośnikach przenośnych,
   c) jako zaszyfrowane pliki w infrastrukturze chmurowej, jeżeli spełnia wymagania bezpieczeństwa.
5) Najlepszą praktyką jest wykonywanie kopii zapasowych zgodnie z zasadą 3-2-1:
   a) 3 kopie (1 produkcyjna + 2 zapasowe),
   b) 2 różne nośniki,
   c) 1 kopia przechowywana poza główną lokalizacją (np. inna część budynku, chmura).
6) Kopie zapasowe są testowane pod kątem możliwości odtworzenia co najmniej raz na rok. Nośniki podlegają regularnej kontroli stanu technicznego i przechowywane są w miejscu zabezpieczonym fizycznie.
7) Procedura odtworzenia danych uruchamiana jest na polecenie dyrektora w przypadku:
   a) utraty danych,
   b) naruszenia integralności danych,
   c) awarii sprzętu lub systemu,
   d) naruszenia bezpieczeństwa (atak, szyfrowanie danych przez złośliwe oprogramowanie).
8) Proces odtworzenia polega na:
   a) wybraniu odpowiedniego punktu przywracania,
   b) odtworzeniu danych,
   c) weryfikacji poprawność danych i działania systemu
   d) poinformowaniu użytkowników o przywróceniu danych.
9) Stare kopie zapasowe są cyklicznie kasowane:
   a) dzienne po 14 dniach,
   b) tygodniowe po miesiącu,

c) archiwalne - zgodnie z Jednolitym Rzeczowym Wykazem Akt.

10) Wszystkie operacje tworzenia, testowania i odtwarzania kopii zapasowych są wpisywane do Rejestru Kopii Zapasowych (Załącznik nr 13).

7. Komunikacja elektroniczna

1) Sprawy służbowe prowadzi się w kanałach zatwierdzonych, zapewniających kontrolę dostępu, możliwość archiwizacji i odtworzenia przebiegu sprawy.
2) Przed przekazaniem danych osobowych przez telefon lub w kanale elektronicznym należy upewnić się, że odbiorca jest uprawniony (np. pytania weryfikujące, odesłanie do kanału oficjalnego w razie wątpliwości).
3) Preferowane kanały komunikacji (od najbardziej rekomendowanych):
   a) dziennik elektroniczny (moduł wiadomości, ogłoszeń, komunikacji z rodzicami),
   b) służbowa poczta e-mail (w domenie placówki),
   c) zatwierdzona platforma edukacyjna (narzędzia wdrożone przez placówkę),
   d) telefon (personel może skontaktować się z rodzicem na numer wskazany w dokumentacji ucznia, ale tylko w uzasadnionych przypadkach).
4) Niedopuszczalne kanały obejmują:
   a) komunikatory internetowe (np. WhatsApp, Messenger) - placówka nie ma kontroli nad tymi narzędziami, co sprawia, że informacje mogą trafić w niepowołane ręce,
   b) prywatne adresy e-mail pracowników (korzystanie z domen komercyjnych) - brak umowy i oficjalnego nadzoru nad taką korespondencją zwiększa ryzyko naruszenia prywatności,
   c) grupy na portalach społecznościowych - nawet jeśli są zamknięte, istnieje ryzyko, że dostęp do nich uzyskają osoby nieuprawnione,
   d) pracownicy nie zapraszają i nie akceptują zaproszeń od uczniów na prywatnych profilach w mediach społecznościowych,

   ze względu na:
   a) brak realnej kontroli administratora nad środowiskiem przetwarzania,
   b) ryzyko nieuprawnionego ujawnienia jest dużo wyższe niż w kanałach oficjalnych,
   c) brak spełnienia wymogów retencji, archiwizacji i odtwarzalności,
   d) trudność realizacji praw osób, których dane dotyczą,
   e) transfer danych (np. poza Europejski Obszar Gospodarczy) i łańcuch podmiotów.

8. Poczta elektroniczna

1) Do celów służbowych używa się wyłącznie służbowego adresu e-mail przydzielonego przez placówkę.
2) W przypadku przesyłania informacji poufnych:
   a) zakres danych ograniczony jest do niezbędnego minimum,
   b) dane umieszcza się w załączniku, nie w treści wiadomości,
   c) załącznik jest zaszyfrowany, a hasło zostaje przekazywane innym kanałem (np. telefonicznie).
3) Przed wysłaniem wiadomości konieczne jest sprawdzenie poprawności adresu odbiorcy.
4) W przypadku wysyłania wiadomości do większej ilości adresatów stosuje się pole UDW/BCC (Ukryte Do Wiadomości), co pozwala zachować prywatność odbiorców, którzy widzą tylko swój adres.

5) Wiadomości zawierające dane osobowe powinny być usuwane po zakończeniu sprawy, chyba że wymagają archiwizacji.
6) W stopce wiadomości umieszcza się co najmniej dane identyfikujące placówkę i link do zakładki klauzul informacyjnych na stronie placówki (załącznik nr 4M).
7) Zabronione jest:
   a) przekazywanie korespondencji służbowej na prywatne skrzynki e-mail,
   b) klikanie podejrzanych linków i otwieranie załączników od nieznanych lub podejrzanych nadawców,
   c) wykorzystywanie poczty służbowej w celach prywatnych.
8) Współdzielenie skrzynki e-mail przez wielu użytkowników (np. sekretariat@...) spełnia wymóg rozliczalności i kontroli dostępu poprzez odpowiednią konfigurację. Każdy użytkownik:
   a) otrzymuje dostęp do wybranych elementów skrzynki (udostępnienie/delegacja folderów skrzynki) ,
   b) otrzymuje określone uprawnienia (odczyt i/lub wysyłka),
   c) loguje się na swoje indywidualne konto, gdzie może dokonywać określonych czynności na wybranych elementach.
9) Użytkownik zgłasza podejrzane wiadomości do dyrektora, IOD lub ASI.

9. Usługi chmurowe

1) Dostęp zdalny do usług chmurowych (np. dziennik elektroniczny, poczta, dysk w chmurze, platformy edukacyjne) odbywa się za pomocą służbowych kont.
2) Logowanie następuje przez oficjalne strony i aplikacje dostawcy.
3) W chmurze przechowuje się wyłącznie dane związane z działalnością placówki.
4) Niedopuszczalne jest używanie prywatnych kont chmurowych do przechowywania danych placówki.
5) Do udostępniania plików z danymi stosuje się bezpieczne metody, np. szyfrowane w chmurze z kontrolą i ograniczonym dostępem do konkretnych osób. Nie używa się niezabezpieczonych kanałów i otwartych plików publicznych widocznych dla wszystkich osób posiadających link.

10. Sztuczna inteligencja (AI)

1) Narzędzia AI to systemy wykorzystujące algorytmy uczenia maszynowego lub generatywne modele językowe zdolne do tworzenia, przekształcania i analizy treści (np. tekst, obraz, dźwięk), podpowiedzi lub automatyzacji zadań na podstawie wprowadzonych danych.
2) Narzędzia AI mogą być wykorzystywane wyłącznie jako wsparcie pracy, w szczególności do:
   a) przygotowywania materiałów dydaktycznych o charakterze ogólnym (propozycje ćwiczeń, przykłady zadań, konspekty),
   b) redagowania i upraszczania treści informacyjnych, ogłoszeń i pism o charakterze ogólnym,
   c) korekty językowej i stylistycznej tekstów,
   d) tłumaczeń treści niezawierających danych osobowych,
   e) generowania pomysłów, struktur dokumentów, zestawień tematycznych,
   f) wsparcia organizacyjnego i planistycznego.
3) Bezwzględnie zabronione jest wykorzystywanie narzędzi AI do:

a) wprowadzania, analizowania lub przetwarzania danych osobowych, danych umożliwiających identyfikację pośrednią, danych poufnych i informacji wewnętrznych,

b) przetwarzania danych szczególnych kategorii (w tym danych o zdrowiu, orzeczeniach, opiniach PPP),

c) działań sprzecznych z prawem oraz naruszających prawa i wolności osób,

d) oceniania osób, przewidywania wyników nauczania lub zachowania,

e) podejmowania decyzji wywołujących skutki prawne lub istotnie wpływających na uczniów lub pracowników,

f) tworzenia profili uczniów lub grup,

g) automatycznego generowania treści zastępujących ocenę merytoryczną,

h) wykorzystywania AI bez wiedzy i kontroli użytkownika (działania autonomiczne),

i) generowania fałszywych informacji lub dokumentów.

4) Użytkownik narzędzi AI ponosi pełną odpowiedzialność za wygenerowane treści, ich zgodność z prawem, podstawą programową i zasadami etyki. Generowane Informacje mają charakter wyłącznie pomocniczy i podlegają krytycznej weryfikacji przed wykorzystaniem - ostateczna decyzja oraz ocena należą do użytkownika.

11. Strona internetowa i media społecznościowe

1) Celem prowadzenia strony internetowej placówki oraz oficjalnego profilu (fanpage) w mediach społecznościowych (np. Facebook, X, Instagram, YouTube) jest:

a) realizacja zadań statutowych o charakterze informacyjnym i promocyjnym,

b) informowanię o działalności placówki,

c) promowanie działalności edukacyjnej i wychowawczej,

d) komunikowanie wydarzeń i osiągnięć,

e) budowanie wizerunku placówki jako instytucji publicznej.

2) Zasady publikacji:

a) treści są zgodne z misją placówki i prawem (w tym prawem autorskim),

b) informacje są rzetelne i aktualne,

c) wpisy nie są wykorzystywane do celów prywatnych, politycznych, komercyjnych lub reklamowych,

d) zabronione jest publikowanie danych osobowych bez podstawy prawnej.

3) Stosowany jest następujący model prowadzenia mediów społecznościowych:

a) oficjalne kanały służą do masowej komunikacji - nie są kanałem do załatwiania spraw indywidualnych,

b) w postach unika się oznaczania profili prywatnych,

c) każda interakcja podlega bieżącej moderacji:

- komentarze zawierające treści obraźliwe, wulgarne, nienawistne, naruszające dobra osobiste lub niezgodne z prawem są niezwłocznie usuwane,
- użytkownicy naruszający zasady są blokowani,

d) w przypadku poważnych naruszeń placówka rozważa czasowe zawieszenie profilu.

4) Platformy społecznościowe posiadają serwery w wielu krajach, co stwarza możliwość transferu danych poza Europejski Obszar Gospodarczy.

12. Korzystanie z urządzeń prywatnych

1) Korzystanie z urządzeń prywatnych do celów służbowych wymaga uprzedniej zgody dyrektora.
2) Użytkownik odpowiada za zapewnienie odpowiednich zabezpieczeń i przestrzegania zasad bezpieczeństwa opisanych w niniejszym SZBI m.in:
   a) stosowanie legalnego i aktualnego oprogramowania,
   b) korzystanie z oprogramowania antywirusowego i zapory sieciowej,
   c) korzystanie z oddzielnego profilu/konta do pracy służbowej, które jest zabezpieczone hasłem,
   d) wydzielenie szyfrowanej przestrzeni służbowej,
   e) automatyczne blokowanie urządzenia przy braku aktywności przez maksymalnie 10 minut,
   f) ograniczenie dostępu do wyświetlanych informacji dla osób postronnych,
3) Należy unikać lokalnego przechowywania informacji służbowych na urządzeniach prywatnych.
4) Urządzenia prywatne mogą być podłączane tylko do sieci gościnnej, chyba że ustalono inaczej z dyrektorem lub ASI.

13. Dostęp zdalny

1) Dostęp do systemów i danych placówki w ramach pracy zdalnej lub dostępu spoza jej siedziby jest dopuszczalny, jeśli został uzgodniony z dyrektorem.
2) Użytkownik zobowiązany jest do:
   a) przestrzeganie zasad bezpieczeństwa opisanych w niniejszym SZBI,
   b) ochrony danych przed dostępem osób nieupoważnionych (np. członków rodziny, osób postronnych),
   c) zabezpieczenia urządzeń i dokumentów przed utratą lub kradzieżą w podróży i miejscu wykonywania zadań (np. przewożenie dokumentów w zamkniętych teczkach, nie pozostawianie zasobów bez nadzoru w zaparkowanym samochodzie),
3) Dostęp zdalny do systemów placówki realizowany jest z wykorzystaniem:
   a) zaufanych sieci internetowych (nie należy korzystać z niezabezpieczonych sieci Wi-Fi),
   b) do infrastruktury lokalnej - poprzez bezpieczne połączenie do sieci placówki (np. VPN z szyfrowaniem, zdalny pulpit),
   c) infrastruktury chmurowej - z użyciem bezpiecznych protokołów szyfrowania (np. HTTPS/TLS, SSH) poprzez oficjalne adresy lub aplikacje dostawców (dziennik elektroniczny, poczta, chmura plików).
4) Po zakończeniu pracy należy wylogować się ze wszystkich systemów i zamknąć połączenie zdalne.

14. Zdalne nauczanie

1) Decyzję o uruchomieniu nauczania zdalnego podejmuje dyrektor, działając zgodnie z przesłankami i trybem określonym w przepisach.
2) Dyrektor komunikuje uruchomienie nauczania zdalnego poprzez dziennik elektroniczny, komunikat na stronie internetowej lub w sposób zwyczajowo przyjęty w placówce. Komunikat zawiera co najmniej: datę startu, przewidywany czas trwania, listę zatwierdzonych narzędzi, zasady kontaktu, zasady obecności/usprawiedliwień, zasady ochrony wizerunku.

3) Placówka prowadzi nauczanie zdalne wyłącznie z użyciem narzędzi zatwierdzonych przez dyrektora, które gwarantują odpowiedni poziom bezpieczeństwa.
4) W przypadku wykorzystania platformy nauczania zdalnego, dostęp odbywa się wyłącznie poprzez konta służbowe (dla pracowników) oraz konta uczniowskie utworzone i zarządzane przez placówkę. Nauczyciel posiada dostęp wyłącznie do grup i zasobów, które prowadzi, a uczeń posiada dostęp jedynie do swoich zajęć.
5) Zajęcia prowadzi się z zastosowaniem następujących ustawień:
   a) włączona poczekalnia lub mechanizm dopuszczania uczestników,
   b) nagrywanie - wyłączone domyślnie,
   c) udostępnianie ekranu - wyłącznie prowadzący (uczniowie tylko na czas i za zgodą nauczyciela),
   d) czat prywatny uczeń-uczeń - wyłączony, a czat grupowy moderowany przez prowadzącego,
   e) linki do spotkań nie są publicznie udostępniane.
6) Weryfikacja obecności odbywa się na podstawie kont użytkowników oraz listy klasowej. Nie żąda się dodatkowych danych identyfikacyjnych.
7) Prowadzący nie wymaga stałego włączania kamery jako warunku uczestnictwa, chyba że jest to chwilowo niezbędne dla realizacji celu dydaktycznego (np. zajęcia praktyczne). W razie potrzeby weryfikacji aktywności stosuje się w pierwszej kolejności mniej inwazyjne metody (odpowiedzi ustne, testy, zadania).
8) Zakazuje się prowadzenia zajęć w sposób umożliwiający osobom postronnym odsłuch/obserwację. Prowadzący zapewnia, aby miejsce prowadzenia zajęć minimalizowało ryzyko ujawnienia danych.
9) Ocenianie i informowanie o wynikach odbywa się poprzez dziennik elektroniczny (preferowany) albo moduł ocen na platformie edukacyjnej.
10) Co do zasady zajęcia zdalne nie są nagrywane. Placówka ogranicza utrwalanie wizerunku i głosu uczniów do sytuacji niezbędnych, w przypadku których:
   a) nagranie ma jednoznacznie określony cel dydaktyczny,
   b) nagranie jest udostępniane wyłącznie z kontrolą dostępu,
   c) okres przechowywania nagrań jest ograniczony do minimum.
11) Uczniom i rodzicom zakazuje się:
   a) nagrywania zajęć, wykonywania zrzutów ekranu oraz ich rozpowszechniania,
   b) publikowania wizerunku/nagrań prowadzących i uczniów w mediach społecznościowych lub innych kanałach.

---

§ 7.

Monitoring wizyjny

1. Postanowienia ogólne

1) Placówka stosuje system monitoringu wizyjnego, który stanowi środek techniczny zwiększający bezpieczeństwo uczniów, pracowników oraz ochronę mienia placówki.
2) Wdrożenie i rozbudowa systemu monitoringu zgodnie z art. 108a ustawy Prawo oświatowe wymaga:
   a) uzgodnienia decyzji z organem prowadzącym,
   b) konsultacji z Radą Pedagogiczną,
   c) konsultacji z Radą Rodziców,

d) konsultacji z Samorządem Uczniowskim,

e) przeprowadzenia analizy ryzyka i oceny skutków dla ochrony danych,

f) poinformowania uczniów i pracowników placówki o fakcie uruchomienia monitoringu w terminie przynajmniej 14 dni przed uruchomieniem.

3) Przed wprowadzeniem systemu dokonano analizy ryzyka oraz rozważono alternatywne, mniej ingerujące środki poprawy bezpieczeństwa. Wobec stwierdzenia, że inne środki są niewystarczające do przeciwdziałania zagrożeniom, zdecydowano o instalacji monitoringu jako środka ostatecznego, proporcjonalnego do zidentyfikowanego ryzyka. Co roku dyrektor dokonuje analizy, czy cele monitoringu są realizowane i czy zakres jest odpowiedni - jeśli zagrożenia się zmniejszyły lub pojawiły się lepsze środki bezpieczeństwa, rozważy ograniczenie lub likwidację kamer.

4) Kamery obejmują tylko te obszary, gdzie występowanie potencjalnych zagrożeń jest istotne (np. wejścia do budynku, korytarze, tereny wokół placówki).

5) Monitoring nie obejmuje pomieszczeń, w których naruszałby prywatność lub godność osób, w tym:

a) pomieszczeń sanitarno-higienicznych (np. toalety),

b) szatni i przebieralni,

c) pokojów nauczycielskich i socjalnych,

d) sal dydaktycznych, wychowawczych i opiekuńczych,

e) gabinetów specjalistycznych (np. pedagoga, psychologa i pielęgniarki).

Objęcie monitoringiem tych wskazanych pomieszczeń może nastąpić wyłącznie wyjątkowo, gdy:

a) istnieje konkrétne i udokumentowane zagrożenie dla bezpieczeństwa osób albo mienia,

b) środek ten jest niezbędny i proporcjonalny,

c) nie narusza godności oraz innych dóbr osobistych osób przebywających w tych pomieszczeniach,

d) zastosowano techniki uniemożliwiające rozpoznanie osób, w szczególności maskowanie lub odpowiednie kadrowanie obrazu,

e) decyzja Dyrektora została odrębnie udokumentowana.

6) Monitoring działa całodobowo. Zapis obrazu odbywa się bez rejestracji dźwięku i nie posiada funkcji rozpoznawania twarzy. Nie stosuje się również atrap kamer - zapobiega to fałszywemu poczuciu nadzoru.

7) System monitoringu w placówce składa się z 23 kamer (budynek 1) i 13 kamer (budynek 2) kamer rozmieszczonych na terenie placówki. Dokładna lokalizacja kamer:

a) **wejścia/wyjścia**: kamera przy głównym wejściu do budynku (obejmuje strefę drzwi wejściowych i fragment holu oraz parkingu), kamera przy bramie wjazdowej, kamera przy wejściu od strony placu apelowego i sali 15 (obejmuje strefę drzwi wejściowych i fragment parkingu), kamera od strony obiektu sportowego i „wejście uczniowskie" (obejmuje strefę drzwi wejściowych),

b) **korytarze**: kamery na korytarzu - parter, I piętro, II piętro obejmujące przestrzenie wspólne przed salami lekcyjnymi, kamera na klatce schodowej,

c) **teren zewnętrzny**: kamery na elewacji budynku skierowane na parking, terem zielony, kamera obejmująca boisko szkolne.

8) Co najmniej raz do roku sprawdza się funkcjonowanie systemu monitoringu: czy wszystkie kamery działają prawidłowo, czy obszar objęty monitoringiem jest prawidłowy, czy obraz jest właściwej jakości, czy zegar systemowy jest zsynchronizowany.

2. Dostęp i udostępnianie

1) Dostęp do podglądu na żywo oraz do archiwalnych nagrań monitoringu mają wyłącznie osoby upoważnione. Dostęp do rejestratorów i serwerów monitoringu ograniczony jest fizycznie i logicznie.

2) Przeglądanie nagrań odbywa się wyłącznie w uzasadnionych przypadkach, tzn. kiedy zaistniało podejrzenie incydentu wymagającego wyjaśnienia (np. kradzież, uszkodzenie mienia, wypadek). Nie praktykuje się rutynowego, codziennego oglądania nagrań bez wyraźnej przyczyny.

3) Udostępnienie nagrań podmiotom zewnętrznym może nastąpić jedynie zgodnie z przepisami prawa. Dotyczy to przede wszystkim:

   a) organów ścigania lub wymiaru sprawiedliwości (policja, prokuratura, sąd) - na ich pisemny wniosek w związku z toczącym się postępowaniem,

   b) rodziców poszkodowanego - w szczególnych przypadkach, gdy nagranie dotyczy zdarzenia z udziałem ich dziecka i może stanowić dowód w dochodzeniu ich praw (np. wypadek, czyn karalny przeciwko dziecku). Dostęp do nagrania realizowany jest poprzez wgląd w obecności upoważnionego pracownika,

   c) innych osób - wgląd w obecności pracownika i tylko w zakresie ich własnych danych osobowych (prawo dostępu przewidziane art. 15 RODO).

   Realizacja prawa dostępu do wizerunku osoby z monitoringu musi jednak uwzględniać prawa i wolności innych osób znajdujących się na nagraniu. Osoby, którym nagranie jest prezentowane nie mogą nagrywać/utrwalać pokazywanego obrazu.

4) Każde udostępnienie odnotowuje się w Rejestrze udostępnień danych osobowych (załącznik nr 5).

3. Okres przechowywania

1) Nagrania są przechowywane przez okres maksymalnie **3 miesięcy** od dnia nagrania. Standardowy okres przechowywania wynosi 14 dni, ale nie dłużej niż 3 miesiące. System jest tak skonfigurowany, że najstarsze nagrania są automatycznie nadpisywane przez nowe po upływie tego okresu (tzw. nadpisywanie cykliczne).

2) W przypadku, gdy nagranie stanowi dowód w postępowaniu prawnym lub placówka powzięła wiadomość, że może stanowić dowód w przyszłości (np. zarejestrowano czyn mogący być przestępstwem, poważne zdarzenie wymagające wyjaśnienia), taki fragment nagrania może zostać zabezpieczony przed nadpisaniem. Zabezpieczenie polega na skopiowaniu nagrania na odrębny nośnik i przechowywaniu go w zabezpieczonym miejscu do czasu prawomocnego zakończenia postępowania związanego z danym zdarzeniem. Po ustaniu potrzeb dowodowych kopia ta zostaje niezwłocznie usunięta.

4. Obowiązek informacyjny

1) Placówka spełniła wobec osób objętych monitoringiem obowiązek informacyjny dotyczący monitoringu. Teren monitorowany jest wyraźnie oznaczony piktogramami i informacjami tekstowymi o monitoringu (załącznik 15B), a szczegółowa klauzula informacyjna (załącznik nr 4J) jest dostępna na stronie internetowej placówki, w widocznym miejscu przy wejściu do budynku oraz w sekretariacie.

2) Regulamin Monitoringu Wizyjnego (załącznik nr 15A) zostaje wprowadzony zarządzeniem dyrektora i udostępniony pracownikom oraz przedstawicielom rodziców i uczniów do wglądu. Jest również dostępny publicznie na stronie internetowej placówki i w sekretariacie placówki jako dokument określający zasady działania monitoringu.

---

§ 8.

Incydenty bezpieczeństwa

1. Zasady postępowania

1) Wszyscy pracownicy, praktykanci, stażyści, wolontariusze oraz podmioty przetwarzające informacje są zobowiązani niezwłocznie zgłosić zauważony incydent bezpieczeństwa do dyrektora lub IOD. Zgłoszenia dokonuje się różnymi kanałami: osobiście, telefonicznie lub e-mail. Powiadomienie powinno zawierać:
   a) opis incydentu,
   b) określenie sytuacji i czasu, w jakim incydent stwierdzono,
   c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę wystąpienia incydentu.
2) Po otrzymaniu zgłoszenia dyrektor we współpracy z IOD i/lub ASI podejmuje natychmiast działania ograniczające skutki incydentu i zabezpieczające dowody. Następnie dokonują wstępnej oceny zdarzenia czy jest to rzeczywisty incydent, jakie zasoby i dane zostały naruszone. Osoba, która pierwsza wykryła incydent, powinna podjąć działania minimalizujące szkody, celem zapobiegnięcia dalszej eskalacji. Przykładowo:
   a) odłączenie zainfekowanego komputera od sieci,
   b) zmiana haseł jeśli wyciekły,
   c) wysłanie prośby o usunięcie wiadomości i nieotwieranie załączników - w przypadku wysłania wiadomości e-mail do błędnego odbiorcy,
   d) zamknięcie drzwi i zabezpieczenie pomieszczeń, w których są przechowywane dokumenty i mogło dojść do nieuprawnionego dostępu,
   e) zamknięcie głównych zaworów wody w przypadku rozszczelnienia instalacji.
3) Dalsze kroki obejmują pełne rozwiązanie problemu m.in.:
   a) ustalenie zakresu ujawnionych informacji i listę osób, których dane dotyczą,
   b) naprawa systemów np. przeinstalowanie systemu z czystej kopii po ataku wirusa,
   c) wymiana uszkodzonego sprzętu,
   d) odzyskanie utraconych danych z kopii zapasowej,
   e) przywrócenie dostępu,
   f) przeniesienie ocalałych akt do suchego miejsca po zalaniu,
4) Wszystkie incydenty są wpisywane do wewnętrznego Rejestru incydentów bezpieczeństwa (załącznik nr 16B).
5) Po opanowaniu skutków incydentu, przeprowadzana jest analiza przyczyn incydentu i podejmowane są działania korygujące, aby zapobiec podobnym zdarzeniom w przyszłości. Może to obejmować dodatkowe szkolenie personelu, zmiana uprawnień, wdrożenie dodatkowych zabezpieczeń, zmiany procedur itp.
6) Wszystkie osoby biorące udział w obsłudze incydentu zobowiązane są traktować sprawę jako poufną i zachować informacje o incydencie w tajemnicy przed niepowołanymi osobami. Ma to na celu m.in. ochronę reputacji placówki oraz

zapobieganie panice czy niekontrolowanemu obiegowi niezweryfikowanych informacji. Publiczne komunikaty o incydencie formułuje wyłącznie dyrektor lub wyznaczona osoba, we współpracy z IOD, aby zapewnić spójność przekazu i nie ujawnić nadmiernych danych.

7) Jeśli incydent dotyczy naruszenia prawa (np. włamanie, kradzież) placówka zawiadamia odpowiednie organy ścigania.

8) W szczególności incydentem bezpieczeństwa jest:
   a) nielegalne ujawnienie danych,
   b) nieautoryzowany dostęp do danych i systemów informatycznych,
   c) nieautoryzowana modyfikacja lub zniszczenie danych,
   d) pozyskiwanie danych z nielegalnych źródeł,
   e) ujawnienie wirusów komputerowych lub ich skutków oraz innych programów naruszających integralność systemu informatycznego,
   f) atak hakerski,
   g) kradzież lub utrata sprzętu IT i dokumentów zawierających dane,
   h) utrata danych na skutek awarii,
   i) wysłanie e-maila z danymi do niewłaściwego odbiorcy,
   j) inne rażące nieprzestrzeganie zasad SZBI lub aktów prawnych regulujących zagadnienia bezpieczeństwa informacji oraz ochrony danych osobowych,
   k) zdarzenia losowe obniżające stan bezpieczeństwa (pożar, zalanie, itp.),
   l) każde zdarzenie, które budzi wątpliwości czy faktycznie jest incydentem podlega zgłoszeniu w celu dokonania wstępnej oceny.

2. Naruszenie ochrony danych osobowych

1) W przypadku stwierdzenia naruszenia ochrony danych osobowych IOD dokonuje oceny charakteru naruszenia i związanych z nim ryzyk dla praw lub wolności osób fizycznych. Na tej podstawie stwierdza, czy naruszenie skutkuje ryzykiem dla osób, których dane dotyczą. Wyniki oceny ryzyka są dokumentowane w Formularzu oceny naruszenia (załącznik nr 16A).

2) Jeżeli zostanie ustalone, że naruszenie może powodować ryzyko dla praw lub wolności osób, dyrektor podejmuje decyzję o zgłoszeniu naruszenia Prezesowi UODO nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Zgłoszenie dokonywane jest za pomocą dedykowanego formularza elektronicznego. Jeśli zgłoszenie nie może być dokonane w ciągu 72 godzin, musi zawierać wyjaśnienie przyczyn opóźnienia.

3) Jeżeli naruszenie może powodować wysokie ryzyko dla praw lub wolności osób, placówka zawiadamia także osoby, których dane dotyczą o zaistniałym naruszeniu. Zawiadomienie następuje bez zbędnej zwłoki opisując w zrozumiałej formie: charakter naruszenia, możliwe konsekwencje, podjęte środki zaradcze, zalecane środki ostrożności oraz przysługujące prawa (załącznik nr 16C). Zawiadomienia dokonuje się poprzez bezpośredni kontakt, w tym: pisemnie, komunikacją elektroniczną lub osobiście z zachowaniem formy pisemnej.

---

§ 9.

Szkolenia i podnoszenie świadomości

1. Postanowienia ogólne

1) Wszyscy pracownicy oraz inne osoby przetwarzające informacje na rzecz placówki są objęci obowiązkowymi szkoleniami z zakresu bezpieczeństwa informacji i ochrony danych osobowych.
2) Za organizację szkoleń odpowiada dyrektor we współpracy z IOD. Program szkoleń jest dostosowany do specyfiki pracy placówki i grupy uczestników. Szkolenia mogą mieć formę stacjonarną lub online.
3) Oprócz formalnych szkoleń, placówka prowadzi bieżące działania uświadamiające: przesyłanie personelowi materiałów przypominających (np. e-maile od IOD o najnowszych zagrożeniach, zasadach cyberbezpieczeństwa), omawianie tematyki ochrony danych na zebraniach z pracownikami.
4) Celem jest utrwalenie kultury ochrony danych w codziennym działaniu placówki.
5) W związku z koniecznością zapewnienia jak najwyższego poziomu szkoleń i monitoringu zgodności IOD zobowiązany jest:
   a) stale rozwijać wiedzę, umożliwiającą pełnienie powierzonej funkcji, w szczególności poprzez uczestnictwo w szkoleniach pozwalających poszerzyć zakres informacji dotyczących procesów związanych z przetwarzaniem danych osobowych,
   b) na bieżąco monitorować zmiany przepisów prawnych regulujących procesy przetwarzania i ochrony danych osobowych.

2. Szkolenia wstępne

1) Pracownik przed dopuszczeniem do pracy z danymi:
   a) odbywa szkolenie wstępne obejmujące bezpieczeństwo danych osobowych i informacji, w szczególności:
      - podstawowe zasady bezpieczeństwa informacji,
      - pojęcia z zakresu ochrony danych osobowych,
      - zasady dostępu do systemów informatycznych,
      - sposób postępowania w przypadku wykrycia incydentów bezpieczeństwa,
      - konsekwencje naruszenia bezpieczeństwa danych,
   b) zapoznaje się z niniejszym SZBI,
   c) podpisuje oświadczenie o zapoznaniu się z obowiązującymi w placówce zasadami bezpieczeństwa informacji i zobowiązuje się do ich przestrzegania.

3. Szkolenia okresowe

1) Szkolenia okresowe realizowane są w cyklu nie rzadszym niż raz na rok lub każdorazowo po istotnej zmianie przepisów lub SZBI.
2) Po każdym szkoleniu uczestnicy wypełniają listę obecności/potwierdzają udział, która przechowywana jest dla celów dowodowych. Placówka może również przeprowadzać krótkie testy wiedzy po szkoleniu, aby upewnić się, że kluczowe wiadomości zostały przyswojone.

---

§ 10.

Zarządzanie ryzykiem

1. Dokumentowanie czynności przetwarzania

1) Placówka prowadzi Rejestr czynności przetwarzania (załącznik nr 17A) oraz Rejestr kategorii czynności przetwarzania (załącznik nr 17B).
2) Za prowadzenie i aktualizację rejestru odpowiada dyrektor we współpracy z IOD.

3) Wszelkie rejestry i ewidencje prowadzone są w formie papierowej lub elektronicznej, według zatwierdzonych wzorów.

2. Analiza ryzyka

1) Placówka prowadzi systematyczną ocenę ryzyka, czyli możliwości wystąpienia zdarzeń mających negatywny wpływ na bezpieczeństwo informacji (załącznik nr 18).
2) Ryzyka są identyfikowane, oceniane i klasyfikowane zgodnie z przyjętą metodyką. Przeglądu dokonuje się co najmniej raz w roku lub w razie zmiany procesów przetwarzania, infrastruktury technicznej, przepisów prawa oraz wystąpienia incydentu bezpieczeństwa.
3) Przy wdrażaniu nowych rozwiązań lub systemów, które wiążą się z przetwarzaniem danych osobowych, placówka stosuje podejście oparte na ochronie danych w fazie projektowania. Oznacza to, że już na etapie planowania każdej operacji lub systemu analizowane są potencjalne ryzyka dla prywatności i podejmowane są stosowne środki, aby zapobiec naruszeniom.
4) Proces zarządzania ryzykiem obejmuje:
   a) identyfikację czynności, celu, kategorii osób i danych, odbiorców oraz istniejących zabezpieczeń - przegląd procesów przetwarzania,
   b) identyfikację zagrożeń i podatności - ustalenie, jakie dane są przetwarzane oraz co im zagraża,
   c) określenie skutków ryzyka,
   d) ocena wartości prawdopodobieństwa wystąpienia i wpływu,
   e) oszacowanie ryzyka wstępnego,
   f) oszacowanie ryzyka resztkowego (rezydualnego) po uwzględnieniu istniejących zabezpieczeń,
   g) ocena akceptowalności ryzyka - kwalifikacja ryzyka jako akceptowalne, nieakceptowalne lub wymagające redukcji,
   h) planowanie działań ograniczenia ryzyka - wybór środków bezpieczeństwa.
5) Dla każdego ryzyka określa się:
   a) skalę prawdopodobieństwa (P) - częstotliwość i warunki sprzyjające:

Wartość	Skala prawdopodobieństwa (P)
1	Incydent mało prawdopodobny (proces lokalny, mała ekspozycja, wąski dostęp)
2	Incydent możliwy sporadycznie (ograniczona liczba użytkowników lub odbiorców)
3	Proces regularny (dane w systemach IT lub obiegu mieszanym, realne ryzyko błędu ludzkiego)
4	Przetwarzanie częste albo rozproszone
5	Wysoka ekspozycja, szczególnie atrakcyjny cel

   b) skalę skutków (S) - maksimum z ocen poufności, integralności, dostępności:

Wartość	Skala skutku / wpływu (S)
1	Krótkotrwała niedogodność, brak trwałych skutków dla osoby i placówki
2	Ograniczone naruszenie prywatności lub pomyłka łatwa do usunięcia
3	Realne utrudnienia, błędna decyzja, zakłócenie pracy lub obowiązek działań naprawczych
4	Poważne naruszenie prywatności, szkoda reputacyjna, finansowa albo edukacyjna

Wartość	Skala skutku / wpływu (S)
5	Szczególnie dotkliwe skutki: długotrwała utrata dostępności, poważne naruszenie danych i realne szkody dla osób, poważne konsekwencje prawne oraz utrata reputacji

6) Na tej podstawie przypisuje się poziom ryzyka:

Macierz oceny ryzyka:

Skutek → Prawdopodobieństwo ↓	1 - Nieznaczny	2 - Mały	3 - Istotny	4 - Poważny	5 - Krytyczny
1 - Bardzo małe	1	2	3	4	5
2 - Małe	2	4	6	8	10
3 - Umiarkowane	3	6	9	12	15
4 - Duże	4	8	12	16	20
5 - Bardzo duże	5	10	15	20	25

Poziomy ryzyka:

Poziom (P×S, Pr x Sr)	Kategoria	Postępowanie
1-4	Niskie	Akceptacja - utrzymanie
5-9	Średnie	Akceptacja warunkowa - monitoring
10-15	Wysokie	Obowiązkowa redukcja ryzyka - zaplanowanie działań redukujących
16-25	Bardzo wysokie	Nieakceptowalne - działanie natychmiastowe, ewentualnie wstrzymanie procesu

7) Postępowanie z ryzykiem:
   a) akceptacja,
   b) ograniczenie (wdrożenie zabezpieczeń),
   c) przeniesienie (np. do dostawcy, ubezpieczenie),
   d) unikanie (zmiana lub wycofanie procesu).

3. Ocena Skutków dla Ochrony Danych (DPIA)

1) Gdy planowane jest rozpoczęcie nowego rodzaju przetwarzania danych mogącego powodować wysokie ryzyko dla praw i wolności (np. wprowadzenie monitoringu wizyjnego, przetwarzanie danych na dużą skalę) placówka przeprowadza ocenę skutków dla ochrony danych (załącznik nr 19 A/B/itd.). Wnioski z oceny są uwzględniane przy podejmowaniu decyzji o wdrożeniu środków bezpieczeństwa.

2) Etapy przeprowadzania DPIA
   a) wstępna analiza - ocena, czy zachodzi konieczność przeprowadzenia DPIA,
   b) opis operacji przetwarzania - czego dotyczy, jakie są cele, jakie dane będą przetwarzane, w jakim zakresie, kogo dotyczą, przez kogo będą zbierane i używane, jak długo przechowywane, kto będzie odbiorcą, czy dane wyjdą poza placówkę lub EOG,
   c) ocena niezbędności i proporcjonalności - analiza pod kątem poszanowania prywatności. Czy planowane środki są niezbędne do osiągnięcia celu i czy nie można go zrealizować inaczej, mniej inwazyjnie. Jeżeli są konieczne, to czy zakres nie jest za szeroki,
   d) ocena ryzyka - zgodnie z metodologią przedstawioną przy analizie ryzyka,

e) środki zaradcze - opis planowanych działań ograniczających ryzyko. Te działania przypisuje się do ryzyka i ocenia resztkowe ryzyko po ich zastosowaniu. Celem jest, by żadne ryzyko nie pozostało wysokie,

f) ocena końcowa - akceptacja poziomu ryzyka. Zwykle, po zastosowaniu odpowiednich środków bezpieczeństwa, ryzyko da się obniżyć do poziomu średniego lub niskiego, co umożliwia wdrożyć nowe rozwiązanie.

3) Przegląd DPIA dokonywany jest przy każdej zmianie charakteru przetwarzania lub pojawienia się nowych zagrożeń.

---

§ 11.

Ciągłość działania

1. Cel i zakres

1) Placówka jest zdolna do utrzymania lub szybkiego wznowienia kluczowych procesów dydaktycznych, opiekuńczych i administracyjnych w przypadku zakłóceń.

2) Procesy krytyczne obejmują:

a) bezpieczeństwo osób,

b) realizację zajęć i opieki,

c) dokumentację przebiegu nauczania,

d) komunikację z rodzicami,

e) obsługę kadrowo-finansową,

f) systemy IT.

2. Role i odpowiedzialność członków Zespołu ds. ciągłości działania

1) Dyrektor - wdrożenie i aktualizacja Planu ciągłości działania, podjęcie decyzji o uruchomieniu procedur awaryjnych, zarządzanie sytuacją kryzysową, wydawanie komunikatów.

2) ASI - zabezpieczanie infrastruktury IT, przywracanie działania systemów IT.

3) Sekretariat - kontakt z rodzicami, dokumentacja awaryjna.

4) IOD - monitorowanie i doradzanie w zakresie oceny zgodności z RODO, nadzór nad dokumentacją incydentu.

3. Ciągłość i odtwarzanie

1) W trybie awaryjnym placówka nie wprowadza obejść, które trwale obniżają bezpieczeństwo informacji, chyba że dyrektor dopuści takie obejście i zastosowano środki kompensacyjne.

2) Decyzje podejmowane są z uwzględnieniem następujących priorytetów (kolejności):

a) bezpieczeństwo osób - zawsze priorytet,

b) utrzymanie minimalnych usług edukacyjnych i opiekuńczych,

c) zabezpieczenie danych i zasobów informacyjnych,

d) odtwarzanie usług.

3) Każdy scenariusz w Planie Ciągłości Działania (załącznik nr 20) zawiera informacje o dopuszczalnym czasie przerwy i alternatywnych sposobów działania oraz instrukcje minimalizujące skutki zakłóceń.

4) Wszystkie poważne zakłócenia są dokumentowane podobnie jak incydenty bezpieczeństwa.