REGON 000214126
SZKOŁA PODSTAWOWA NR 10
im. Komisji Edukacji Narodowej
w Toruniu, ul. Bażyńskich 30/36
tel. 56 6557150 NIP 8792287003

Załącznik nr 1 do Zarządzenia Dyrektora Szkoły 15/2026 z dn. 2.06.26

POLITYKA BEZPIECZEŃSTWA INFORMACJI

w Szkole Podstawowej nr 10 im. Komisji Edukacji Narodowej w Toruniu.

Postanowienia ogólne

1. Polityka Bezpieczeństwa Informacji (dalej: „Polityka") określa zasady, środki i odpowiedzialności związane z zapewnieniem bezpieczeństwa informacji przetwarzanych w Publicznej Szkole Podstawowej nr 10 im. Komisji Edukacji Narodowej w Toruniu (dalej: „Szkoła").
2. Polityka ma na celu zapewnienie poufności, integralności i dostępności informacji, w szczególności danych osobowych uczniów, rodziców, pracowników i kontrahentów.
3. Administratorem danych osobowych jest Szkoła Podstawowa nr 10 im. Komisji Edukacji Narodowej w Toruniu, reprezentowana przez Dyrektora Szkoły.

Podstawa prawna

1. Niniejsza Polityka została opracowana na podstawie:
   - rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO);
   - ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
   - ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
   - rozporządzenia z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (KRI);
   - ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe;
   - innych aktów prawnych regulujących funkcjonowanie jednostek sektora finansów publicznych oraz publicznych szkół.

Zakres stosowania

1. Polityka obowiązuje:
   - Dyrektora szkoły;
   - nauczycieli;
   - pracowników administracji i obsługi;
   - osoby współpracujące na podstawie umów cywilnoprawnych.
2. Podmioty zewnętrzne świadczące usługi na rzecz Szkoły w zakresie przetwarzania informacji (np. e-dziennik, hosting, serwis urządzeń).

Cele bezpieczeństwa informacji

1. Celem Polityki jest:
   - zapewnienie zgodnego z prawem przetwarzania danych osobowych;
   - ochrona informacji przed nieuprawnionym dostępem, utratą, zniszczeniem lub ujawnieniem;
   - zapewnienie ciągłości działania podstawowych procesów edukacyjnych i administracyjnych;
   - ograniczanie ryzyk związanych z cyberbezpieczeństwem w środowisku szkolnym.

Role i odpowiedzialności

1. Dyrektor szkoły:
   - odpowiada za nadzór nad zapewnieniem bezpieczeństwa informacji i wdrożenie niniejszej Polityki;
   - wydaje upoważnienia do przetwarzania danych osobowych;
   - zatwierdza procedury i instrukcje.

2. Inspektor Ochrony Danych (IOD):
   - monitoruje przestrzeganie przepisów RODO i niniejszej Polityki;
   - prowadzi rejestry i dokonuje oceny ryzyk;
   - doradza Dyrektorowi w zakresie ochrony danych;
   - punkt kontaktowy dla organu nadzorczego i osób, których dane dotyczą.

3. Nauczyciele i pracownicy:
   - przetwarzają dane zgodnie z upoważnieniami i instrukcjami;
   - zabezpieczają informacje zgodnie z niniejszą Polityką;
   - zgłaszają incydenty naruszenia ochrony danych.

4. Podmioty przetwarzające:
   - przetwarzają dane na podstawie umowy powierzenia zgodnie z art. 28 RODO.

Otoczenie organizacyjne

1. Szkoła działa jako jednostka organizacyjna jednostki samorządu terytorialnego – Miasta Toruń, którego organem prowadzącym jest Prezydent Miasta Torunia. Prezydent wykonuje zadania związane z zapewnieniem właściwych warunków organizacyjnych i finansowych funkcjonowania Szkoły, w tym infrastruktury technicznej niezbędnej do przetwarzania informacji.
2. Szkoła podlega nadzorowi pedagogicznemu Kuratora Oświaty oraz nadzorowi pracowniczemu organu prowadzącego w zakresie zgodności swojej działalności z przepisami prawa.
3. Administratorem danych osobowych przetwarzanych w szkole jest Dyrektor szkoły. Organ prowadzący nie jest administratorem danych gromadzonych i przetwarzanych przez szkołę, chyba że przetwarzanie danych wynika z realizacji odrębnych obowiązków ustawowych (np. nadzór pracowniczy, finanse publiczne, kontrola zarządcza).
4. IOD pełni funkcję zgodnie z art. 37–39 RODO i jest wyznaczony przez organ prowadzący w ramach Centrum Usług Wspólnych.
5. Przetwarzanie danych osobowych odbywa się w następujących obszarach organizacyjnych:
   - sekretariat szkoły;
   - gabinet pedagoga/psychologa;
   - księgowość (organizacyjnie prowadzona przez szkołę lub wspólny referat w urzędzie miasta);
   - biblioteka szkolna;
   - dzienniki elektroniczne i systemy informatyczne używane przez nauczycieli;
   - gabinet dyrektora.
6. Szkoła może przetwarzać dane osobowe przy pomocy podmiotów zewnętrznych na podstawie umowy powierzenia, w szczególności:
   - dostawców systemu dziennika elektronicznego;

- dostawców hostingu poczty elektronicznej i usług chmurowych;
- firm serwisujących sprzęt komputerowy;
- firm realizujących usługi związane z archiwizacją i niszczeniem dokumentacji;
- firm szkoleniowych i doradczych;
- podmiotów prowadzących bezpłatne programy edukacyjne finansowane ze środków publicznych.

7. Szkoła stosuje model zarządzania systemem informatycznym zgodny z Krajowymi Ramami Interoperacyjności (KRI), w szczególności w zakresie:
   - stosowania kontroli dostępu;
   - prowadzenia rejestrów osób upoważnionych;
   - zarządzania incydentami;
   - stosowania zasad retencji i archiwizacji.
8. Szkoła funkcjonuje w środowisku zwiększonego ryzyka cyberbezpieczeństwa, w szczególności z uwagi na:
   - korzystanie z usług chmurowych i e-dziennika;
   - przetwarzanie danych szczególnych kategorii dotyczących uczniów;
   - ograniczone możliwości kadrowe w obszarze IT;
   - korzystanie z urządzeń przenośnych i dostęp do Internetu przez wiele osób (nauczyciele, uczniowie, pracownicy).

Klasyfikacja informacji

1. W szkole wyróżnia się następujące kategorie informacji:
   - informacje jawne (np. ogłoszenia szkolne, publikacje na stronie szkoły);
   - informacje służbowe (np. notatki służbowe, korespondencja wewnętrzna);
   - dane osobowe zwykłe (uczniowie, rodzice, pracownicy);
   - dane szczególnej kategorii (np. informacje o stanie zdrowia dzieci, z opinii poradni psychologiczno-pedagogicznej, dane dotyczące orzeczeń o kształceniu specjalnym).

Uprawnienia i zarządzanie dostępem

1. Dostęp do informacji i danych osobowych jest nadawany zgodnie z zasadą minimalnych uprawnień niezbędnych do wykonywania obowiązków służbowych.
2. Nadawanie i odbieranie uprawnień dokumentowane jest w Rejestrze osób upoważnionych prowadzonym przez Dyrektora Szkoły lub osobę upoważnioną.
3. Uprawnienia do systemów informatycznych są niezwłocznie usuwane po ustaniu zatrudnienia lub zmiany stanowiska wymagającej mniejszego zakresu dostępu.

Zasady bezpieczeństwa informacji

1. Informacje papierowe przechowywane są w zamykanych pomieszczeniach lub szafach, dostępnych wyłącznie dla osób upoważnionych.
2. Dokumenty zawierające dane osobowe nie mogą być pozostawiane w miejscach dostępnych dla osób postronnych.
3. Dokumentacja archiwalna podlega okresowej selekcji i niszczeniu przy użyciu niszczarki.

Analiza ryzyka

1. Szkoła przeprowadza analizę ryzyka dla bezpieczeństwa informacji w oparciu o odrębną Procedurę Analizy Ryzyka dla Bezpieczeństwa Informacji, zatwierdzoną przez Dyrektora Szkoły.
2. Analiza ryzyka obejmuje identyfikację zagrożeń, ocenę ryzyka oraz wdrożenie działań ograniczających ryzyko do poziomu akceptowalnego.
3. Analiza ryzyka wykonywana jest nie rzadziej niż raz w roku oraz każdorazowo w przypadku wystąpienia istotnej zmiany organizacyjnej lub technicznej w zakresie przetwarzania informacji, a także po wystąpieniu incydentu bezpieczeństwa.
4. Wyniki analizy ryzyka są dokumentowane i stanowią podstawę do aktualizacji niniejszej Polityki oraz innych dokumentów związanych z bezpieczeństwem informacji.

Ciągłość działania

1. Szkoła zapewnia ciągłość działania w zakresie przetwarzania informacji w oparciu o odrębną Procedurę ciągłości działania, zatwierdzoną przez Dyrektora szkoły.
2. Procedura obejmuje w szczególności:
   - opracowanie Planu ciągłości działania (PCD) dla kluczowych procesów związanych z przetwarzaniem informacji;
   - wskazanie osób odpowiedzialnych za realizację PCD;
   - zasady odtwarzania danych oraz przywracania dostępu do systemów informatycznych.
3. Plan ciągłości działania jest testowany nie rzadziej niż raz w roku oraz każdorazowo po istotnej zmianie organizacyjnej lub technicznej.
4. Wyniki testów i ewentualne działania korygujące dokumentowane są w formie Protokołu testów ciągłości działania i stanowią podstawę do aktualizacji Planu ciągłości działania oraz procedury.

Zasady bezpieczeństwa systemów informatycznych

1. Komputery, na których przetwarzane są dane, zabezpiecza się hasłem spełniającym minimalne wymagania określone w instrukcji zarządzania systemem informatycznym.
2. Urządzenia przenośne (np. pendrive) mogą być używane wyłącznie po uzyskaniu zgody Dyrektora.
3. System e-dziennika może być wykorzystywany wyłącznie przez osoby upoważnione, mające indywidualne loginy i hasła.
4. Szkoła korzysta wyłącznie z oprogramowania posiadającego legalną licencję.
5. Prowadzone są regularne kopie zapasowe danych elektronicznych.
6. Szkoła zapewnia rejestrowanie dostępu do systemów informatycznych oraz przechowywanie logów dostępowych przez okres umożliwiający analizę zdarzeń naruszenia bezpieczeństwa.

Udostępnianie danych osobowych

1. Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym na podstawie przepisów prawa (np. sąd, policja, organ prowadzący, kuratorium oświaty).
2. Udostępnianie danych innym podmiotom wymaga zgody Dyrektora oraz zawarcia umowy powierzenia, jeśli wynika ona z art. 28 RODO.

3. Dane osobowe przesyła się w sposób zabezpieczony, w szczególności poprzez szyfrowanie wiadomości e-mail lub stosowanie haseł do plików.

Zgłaszanie incydentów

1. Każdy pracownik ma obowiązek niezwłocznego zgłaszania naruszenia ochrony danych osobowych do Dyrektora i IOD.
2. Postępowanie w przypadku naruszenia ochrony danych osobowych oraz incydentów bezpieczeństwa informacji odbywa się zgodnie z odrębną Procedurą zgłaszania i obsługi incydentów bezpieczeństwa informacji.
3. Dyrektor dokonuje analizy naruszenia i decyduje o obowiązku zgłoszenia naruszenia Prezesowi UODO oraz poinformowania osób, których dane dotyczą.

Szkolenia

1. Pracownicy, nauczyciele oraz osoby mające dostęp do danych osobowych są szkolone w zakresie ochrony danych osobowych przed dopuszczeniem do przetwarzania danych osobowych, a następnie co najmniej raz na dwa lata.
2. Szkolenia dokumentowane są w formie protokołów lub list obecności.

Przegląd i aktualizacja Polityki

1. Polityka podlega przeglądowi co najmniej raz na 12 miesięcy albo wcześniej, jeśli wymagają tego zmiany organizacyjne, technologiczne lub prawne.
2. Za przegląd odpowiedzialny jest Dyrektor w porozumieniu z Inspektorem Ochrony Danych.

Mierzenie skuteczności Systemu Zarządzania Bezpieczeństwem Informacji

1. Szkoła zapewnia systematyczną ocenę skuteczności działań w zakresie bezpieczeństwa informacji oraz realizacji wymagań niniejszej Polityki.
2. Mierzenie skuteczności obejmuje co najmniej następujące obszary:
   - przestrzeganie zasad ochrony danych przez pracowników i nauczycieli;
   - poprawność i aktualność nadawania oraz odbierania upoważnień do przetwarzania danych;
   - terminowość zgłaszania incydentów naruszenia ochrony danych;
   - realizację obowiązków informacyjnych wobec rodziców, uczniów i pracowników;
   - aktualność umów powierzenia przetwarzania danych z podmiotami zewnętrznymi;
   - poprawność i aktualność prowadzenia e-dziennika i innych systemów informatycznych wykorzystywanych do przetwarzania danych.
3. Monitoring skuteczności obejmuje prowadzenie i analizę co najmniej następujących wskaźników:
   - liczba przeprowadzonych szkoleń z ochrony danych osobowych;
   - liczba zgłoszonych incydentów bezpieczeństwa informacji w danym okresie;
   - liczba stwierdzonych naruszeń zasad przetwarzania danych osobowych podczas kontroli wewnętrznych;
   - liczba zawartych i zaktualizowanych umów powierzenia przetwarzania danych;
   - liczba zgłoszeń rodziców lub pracowników dotyczących nieprawidłowości w zakresie przetwarzania danych;
   - liczba wymuszonych zmian haseł i blokad kont użytkowników systemów szkolnych.

4. IOD przedstawia Dyrektorowi szkoły, nie rzadziej niż raz w roku, krótkie sprawozdanie z monitorowania skuteczności SZBI, zawierające:
   - wyniki pomiarów;
   - ocenę trendów (np. wzrost / spadek incydentów);
   - rekomendacje działań korygujących;
   - wykaz obszarów wymagających poprawy.
5. Dyrektor szkoły podejmuje działania korygujące lub zapobiegawcze wynikające ze sprawozdania IOD, w szczególności poprzez:
   - organizację dodatkowych szkoleń;
   - aktualizację Polityki;
   - przegląd i aktualizację upoważnień;
   - przegląd i aktualizację procedur, instrukcji oraz umów powierzenia.
6. W ramach mierzenia skuteczności SZBI przeprowadza się co najmniej raz w roku przegląd bezpieczeństwa informacji, obejmujący:
   - analizę ryzyka;
   - weryfikację aktualności środków technicznych i organizacyjnych;
   - ocenę aktualności dokumentacji.
7. Wyniki pomiarów, rekomendacje IOD oraz decyzje Dyrektora dokumentowane są w Protokole przeglądu SZBI, który podlega archiwizacji przez okres co najmniej 5 lat.

Bezpieczeństwo systemów teleinformatycznych (zgodność z KRI)

1. Szkoła realizuje wymagania określone w KRI.
2. Szkoła zapewnia bezpieczeństwo informacji przetwarzanych w systemach teleinformatycznych, w szczególności poprzez stosowanie następujących środków organizacyjnych i technicznych:
   1) zarządzanie dostępem:
      - nadawanie uprawnień na podstawie upoważnień do przetwarzania danych;
      - kontrolę dostępu opartą o indywidualne identyfikatory użytkowników;
      - stosowanie haseł o odpowiednim poziomie złożoności oraz regularną ich zmianę;
      - blokowanie kont w przypadku nieużywania lub ustania podstawy przetwarzania.
   2) zabezpieczenie systemów i urządzeń:
      - stosowanie aktualizowanego oprogramowania antywirusowego i firewall;
      - bieżącą aktualizację systemów operacyjnych i aplikacji;
      - instalowanie poprawek bezpieczeństwa (update/patch management).
   3) ochronę przed utratą danych:
      - wykonywanie regularnych kopii zapasowych danych;
      - przechowywanie kopii w sposób zabezpieczający przed utratą i nieuprawnionym dostępem;
      - testowanie przywracania danych z kopii zapasowych nie rzadziej niż raz na rok.
   4) zarządzanie incydentami:
      - prowadzenie rejestru incydentów naruszenia bezpieczeństwa informacji;
      - analizę przyczyn i skutków incydentów;
      - stosowanie działań naprawczych i zapobiegawczych.
3. Szkoła zapewnia ciągłość działania systemów teleinformatycznych, w szczególności systemu dziennika elektronicznego, poczty elektronicznej i dokumentacji szkolnej, poprzez:

- stosowanie mechanizmów odtworzeniowych (backup);
- wyznaczenie osób odpowiedzialnych za przywrócenie dostępu do danych w przypadku awarii;
- dokumentowanie działań awaryjnych (karty zgłoszeń, protokoły).

4. Szkoła współpracuje z organem prowadzącym w zakresie:
   - zapewnienia infrastruktury technicznej;
   - zabezpieczenia sieci komputerowej;
   - bieżącego serwisu systemów i urządzeń;
   - realizacji obowiązków wynikających z KRI, w szczególności aktualizacji systemów teleinformatycznych i wykonywania kopii zapasowych.
5. Szkoła prowadzi okresową analizę ryzyka utraty bezpieczeństwa informacji zgodnie z KRI, obejmującą:
   - identyfikację zagrożeń i podatności;
   - ocenę prawdopodobieństwa ich wystąpienia;
   - ocenę wpływu na poufność, integralność i dostępność danych;
   - wyznaczenie planów działań minimalizujących ryzyko.
6. Dyrektor szkoły lub osoba wyznaczona dokonuje przeglądu zgodności z wymaganiami KRI co najmniej raz w roku oraz w przypadku:
   - zmiany systemów informatycznych;
   - zmiany administratorów systemów;
   - wystąpienia incydentu bezpieczeństwa informacji.
7. Wyniki przeglądu zgodności KRI dokumentowane są w Raporcie z przeglądu KRI, który zatwierdza Dyrektor szkoły i przechowuje przez okres co najmniej 5 lat.

Korzystanie z urządzeń prywatnych i nośników danych

1. Korzystanie przez pracowników i nauczycieli z prywatnych urządzeń (laptopów, telefonów, tabletów, pendrive) do celów służbowych wymaga zgody Dyrektora Szkoły i odbywa się zgodnie z odrębną Procedurą korzystania z urządzeń prywatnych.
2. Zabrania się przechowywania danych osobowych na prywatnych nośnikach danych, chyba że uzyskano pisemną zgodę Dyrektora i zastosowano środki zabezpieczeń, w tym szyfrowanie.
3. Urządzenia prywatne używane do celów służbowych muszą być zabezpieczone hasłem oraz oprogramowaniem antywirusowym.
4. Szkoła zastrzega sobie prawo do weryfikacji, czy urządzenie prywatne wykorzystywane do przetwarzania danych spełnia wymagania techniczne określone w Procedurze korzystania z urządzeń prywatnych.

Retencja i niszczenie dokumentów

1. Czas przechowywania dokumentów zawierających dane osobowe jest zgodny z Jednolitym Rzeczowym Wykazem Akt (JRWA) obowiązującym w Szkole.
2. Niszczenie dokumentacji zawierającej dane osobowe odbywa się zgodnie z odrębną Procedurą niszczenia dokumentów.
3. Niszczenie dokumentów odbywa się przy użyciu niszczarki o klasie bezpieczeństwa co najmniej DIN 66399 P-4 lub poprzez usługę zewnętrzną na podstawie umowy powierzenia danych.

Wykaz systemów informatycznych

1. Szkoła prowadzi Wykaz systemów informatycznych oraz usług przetwarzania danych osobowych, obejmujący w szczególności:
   - dziennik elektroniczny;
   - system poczty elektronicznej;
   - program kadrowo-płacowy (jeśli dotyczy);
   - system biblioteczny;
   - system do komunikacji z rodzicami;
   - zewnętrzne platformy edukacyjne wykorzystywane w procesie nauczania;
   - System informacji oświatowej;
   - Rejestr sprawców przestępstw na tle seksualnym.
2. Wykaz systemów stanowi załącznik do niniejszej Polityki i jest aktualizowany nie rzadziej niż raz w roku.

Kopie zapasowe i odtwarzanie danych

1. Szkoła wykonuje regularne kopie zapasowe danych przetwarzanych w systemach teleinformatycznych zgodnie z Procedurą wykonywania kopii zapasowych.
2. Kopie zapasowe przechowuje się w sposób uniemożliwiający ich utratę lub dostęp osób nieuprawnionych.
3. Test przywracania danych z kopii zapasowych przeprowadza się nie rzadziej niż raz w roku, a wynik testu dokumentuje w protokole.

Komunikacja elektroniczna i narzędzia zdalne

1. Korzystanie z komunikatorów elektronicznych, wideokonferencji, e-learningu i narzędzi zdalnych wymaga stosowania zasad określonych w odrębnej Procedurze korzystania z narzędzi online.
2. Zabrania się wykorzystywania prywatnych kont poczty elektronicznej do celów służbowych związanych z przetwarzaniem danych osobowych.
3. Konta w serwisach edukacyjnych (np. Teams, Zoom, Google Classroom, Librus, Vulcan) muszą być zabezpieczone unikalnym hasłem.

Odpowiedzialność za naruszenie postanowień Polityki

1. Pracownicy, nauczyciele oraz osoby wykonujące na rzecz Szkoły czynności związane z przetwarzaniem informacji są zobowiązani do przestrzegania postanowień niniejszej Polityki oraz powiązanych procedur i instrukcji w zakresie bezpieczeństwa informacji.
2. Naruszenie postanowień Polityki oraz powiązanych procedur może stanowić naruszenie obowiązków pracowniczych, skutkujące odpowiedzialnością porządkową, dyscyplinarną lub innymi konsekwencjami przewidzianymi przepisami prawa pracy, ustawy — Prawo oświatowe oraz przepisami wewnętrznymi szkoły.
3. W przypadku stwierdzenia naruszenia Polityki mającego wpływ na bezpieczeństwo danych osobowych, Dyrektor szkoły może:
   - cofnąć upoważnienie do przetwarzania danych;
   - ograniczyć zakres dostępu do informacji;
   - zobowiązać do odbycia dodatkowego szkolenia w zakresie ochrony danych osobowych i bezpieczeństwa informacji.

4. W przypadku rażącego naruszenia obowiązków w zakresie ochrony danych osobowych lub bezpieczeństwa informacji, Dyrektor szkoły może podjąć działania przewidziane przepisami prawa, w tym:
   - nałożyć kary przewidziane Kodeksem pracy;
   - wystąpić z wnioskiem o wszczęcie postępowania dyscyplinarnego nauczyciela;
   - zawiadomić odpowiednie organy nadzoru lub organy ścigania.
5. Podmioty zewnętrzne przetwarzające dane na podstawie umowy powierzenia ponoszą odpowiedzialność za naruszenie Polityki oraz powiązanych procedur zgodnie z postanowieniami umowy powierzenia oraz przepisami RODO.
6. Osoby, które powzięły informację o naruszeniu postanowień Polityki, są zobowiązane do niezwłocznego zgłoszenia tego faktu Dyrektorowi Szkoły lub Inspektorowi Ochrony Danych.

DYREKTOR
SZKOŁY PODSTAWOWEJ NR 10
im. Komisji Edukacji Narodowej
w Toruniu
mgr Iwona Cieślak