ZESPOŁ SZKÓŁ ELEKTRYCZNYCH
im. prof. Janusza Groszkowskiego
15-111 BIAŁYSTOK
ul. 1000 Lecia Państwa Polskiego 14
tel. 85 65 12 174, 000185376

Zarządzenie Nr ...71.../26/27

Dyrektora

Zespołu Szkół Elektrycznych im. prof. Janusza Groszkowskiego w Białymstoku

z dnia 19 listopada 2026 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Zespole Szkół Elektrycznych im. prof. Janusza Groszkowskiego w Białymstoku

Na podstawie art. 68 ust. 1 pkt 7 ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe (t.j. Dz.U. z 2026 r. poz. 820 ze zm.) w związku z art. 8 ust. 1 pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 ze zm.) zarządza się, co następuje:

§ 1

Ustala się Politykę Bezpieczeństwa Informacji w Zespole Szkół Elektrycznych im. prof. Janusza Groszkowskiego w Białymstoku, zwaną dalej Polityką, jako podstawę funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji, w brzmieniu stanowiącym załącznik do niniejszego zarządzenia. Wdrożenie dokumentu ma na celu określenie zasad przetwarzania informacji gwarantujących odpowiedni poziom bezpieczeństwa oraz zgodność z obowiązującymi przepisami prawa.

§ 2

Poprzez wprowadzenie Polityki wyraża się wolę pełnego zaangażowania dla zapewnienia bezpieczeństwa przetwarzanych informacji oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z bezpieczeństwem informacji.

§ 3

Polityka obowiązuje wszystkich pracowników oraz inne osoby wykonujące pracę na rzecz *Zespołu Szkół Elektrycznych im. prof. Janusza Groszkowskiego w Białymstoku.*

§ 4

Zarządzenie wchodzi w życie z dniem ogłoszenia.

DYREKTOR
ZESPOŁU SZKÓŁ ELEKTRYCZNYCH
mgr inż. Anna Niczyporuk

Załącznik Nr 1
do zarządzenia Nr 11./26/27
Dyrektora Zespołu Szkół Elektrycznych
im. prof. Janusza Groszkowskiego w Białymstoku

z dnia 19 listopada 2026 r.

Polityka Bezpieczeństwa Informacji w Zespole Szkół Elektrycznych im. prof. Janusza Groszkowskiego w Białymstoku

Podstawowym celem Zespołu Szkół Elektrycznych im. prof. Janusza Groszkowskiego w Białymstoku jest wychowanie, kształcenie, opieka oraz rozwój społeczny i kulturowy dzieci. Cele te są związane z bezpieczeństwem informacji, a w szczególności z cyberbezpieczeństwem, którego zapewnienie stanowi realny problem współczesnej rzeczywistości. Dążąc do zapewnienia jak najlepszej jakości usług oraz bezpieczeństwa danych uczniów, rodziców, pracowników i innych osób wykonujących usługi na rzecz Zespołu Szkół Elektrycznych im. prof. Janusza Groszkowskiego w Białymstoku, a także wszystkich innych zainteresowanych osób, wprowadza się niniejszą Politykę Bezpieczeństwa Informacji w Zespole Szkół Elektrycznych im. prof. Janusza Groszkowskiego w Białymstoku.

§1. ZAKRES STOSOWANIA

1. Polityka bezpieczeństwa informacji w Zespole Szkół Elektrycznych im. prof. Janusza Groszkowskiego w Białymstoku, zwana dalej Polityką, ma zastosowanie przy przetwarzaniu informacji przez Zespół Szkół Elektrycznych im. prof. Janusza Groszkowskiego w Białymstoku :
   1) w jej systemie informatycznym;
   2) w prowadzonej przez nią dokumentacji papierowej;
   3) w usługach dostarczanych przez dostawców usług;
2. Polityka obowiązuje wszystkich pracowników, stażystów, praktykantów, wolontariuszy oraz inne osoby wykonujące prace na rzecz lub w imieniu Zespołu Szkół Elektrycznych im. prof. Janusza Groszkowskiego w Białymstoku.
3. Polityka nie ma zastosowania do:
   1) naruszeń ochrony danych osobowych procedowanych na podstawie przepisów o ochronie danych osobowych, niebędących jednocześnie incydentami bezpieczeństwa informacji;

2) zarządzania informacjami niejawnymi przetwarzanymi na podstawie przepisów o ochronie informacji niejawnych.

§2. SŁOWNICZEK POJĘĆ

Użyte w niniejszej Polityce określenia oznaczają:

1) **Jednostka** - rozumie się przez to Zespół Szkół Elektrycznych im. prof. Janusza Groszkowskiego w Białymstoku;
2) **Pracownik** – osoba wykonującą pracę na rzecz Jednostki na podstawie umowy o pracę, pozaumownych stosunków pracy, umowy zlecenia lub umowy o dzieło;
3) **SZBI** - System Zarządzania Bezpieczeństwem Informacji w Zespole Szkół Elektrycznych im. prof. Janusza Groszkowskiego w Białymstoku, na który składają się zestaw polityk, procesów zarządzania, procedur oraz narzędzi chroniących informacje w Jednostce;
4) **cyberzagrożenie** - wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób;
5) **incydent** - zdarzenie lub ciąg zdarzeń, który ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemu informatycznego Jednostki;
6) **system informatyczny Jednostki** – oznacza funkcjonujący w Jednostce zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego.

§3. ROLA POLITYKI

Polityka jest podstawowym i nadrzędnym dokumentem Systemu Zarządzania Bezpieczeństwem Informacji. Pozostałe dokumenty wytworzone w procesie wprowadzania SZBI są dokumentami wykonawczymi do Polityki, wynikają z niej i nie mogą pozostawać z jej zapisami w sprzeczności. Dokument ustala ramy zarządzania bezpieczeństwem informacji zgodnie z obowiązującymi przepisami prawnymi, zwłaszcza z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2026 r., poz. 20, ze zm.).

§4. DEKLARACJA DYREKTORA JEDNOSTKI

Dyrektor Jednostki postanawia utrzymywać SZBI w zgodności z Polityką, w tym:

1) ustanawia cele bezpieczeństwa informacji i zapewnia ich zgodność z kierunkiem strategicznym Jednostki;
2) włącza zasady określone w SZBI w codzienną praktykę funkcjonowania Jednostki;
3) zapewnia zasoby materialne, informacyjne i osobowe do skutecznego funkcjonowania SZBI;
4) komunikuje znaczenie przestrzegania wymagań SZBI;
5) zapewnia, że SZBI osiąga zamierzone wyniki;
6) kieruje Pracownikami i wspiera ich w działaniach zapewniających skuteczne funkcjonowanie SZBI;
7) promuje ciągłe doskonalenie;
8) przydziela i nadzoruje wykonywanie obowiązków z zakresu cyberbezpieczeństwa przez wyznaczone osoby mu podległe;
9) zapewnia Pracownikom dostęp do wiedzy, pozwalającej na zrozumienie zjawiska cyberzagrożeń i stosowania skutecznych sposobów zabezpieczania się przed nimi;
10) wyznacza odpowiedni poziom zabezpieczenia informacji, zgodnie z zasadami poufności, integralności, dostępności i autentyczności danych, przy zachowaniu możliwości wykazania ich przestrzegania.

§5. PRZYPISANIE RÓL I ODPOWIEDZIALNOŚCI

1. Dyrektor Jednostki jest kierownikiem podmiotu ważnego, w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2026 r., poz. 20, ze zm.), co oznacza, że ponosi odpowiedzialność za wykonywanie obowiązków w zakresie cyberbezpieczeństwa, o których mowa w powyższej ustawie, także wtedy, gdy niektóre z obowiązków albo wszystkie obowiązki powierzył innej osobie za jej zgodą.
2. Dyrektor Jednostki wyznacza co najmniej dwie osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, zgodnie z art. 9 ust. 1 pkt 1 ww. ustawy.
3. Dyrektor Jednostki wyznacza co najmniej jedną osobę odpowiedzialną za utrzymywanie kontaktów z innymi podmiotami kluczowymi lub podmiotami ważnymi, zgodnie z art. 9 ust. 3 ww. ustawy.
4. Za administrowanie, kontrolowanie oraz bieżące utrzymanie systemu informatycznego Jednostki odpowiada informatyk.

5. Każdy Pracownik jest odpowiedzialny za przestrzeganie zasad SZBI, zgodnie z zakresem powierzonych mu zadań.

§6. CELE SZBI

SZBI musi spełniać następujące cele:

1) zapewnienie niezakłóconego świadczenia usług przez Jednostkę;
2) zapewnienie poufności, dostępności, integralności i autentyczności informacji przetwarzanych w Jednostce;
3) zabezpieczenie danych przed nieuprawnionym dostępem, modyfikacją, ujawnieniem lub zniszczeniem;
4) ochrona systemu informatycznego Jednostki przed atakami, błędami, awariami lub działaniem sił natury;
5) zapewnienie ciągłości działania Jednostki;
6) zapewnienie zgodności dokumentacji z regulacjami ustawowymi;
7) umożliwienie, dzięki zawartym w SZBI regulacjom, procesu ciągłego doskonalenia funkcjonowania systemu informatycznego Jednostki;
8) podnoszenie świadomości Pracowników Jednostki o cyberzagrożeniach oraz zachęcanie ich do stosownego reagowania i zgłaszania potencjalnie niebezpiecznych zdarzeń.

§7. NIEZBĘDNE OBSZARY ZARZĄDZANIA BEZPIECZEŃSTWEM

SZBI powinien obejmować swoim zakresem regulacyjnym co najmniej:

1) inwentaryzowanie oraz ciągłe monitorowanie środków służących do bezpiecznego przetwarzania danych celem ich ciągłego doskonalenia oraz zapewnienia ciągłości działania systemu informatycznego Jednostki;
2) zapewnienie odpowiedniego poziomu zabezpieczenia informacji, zgodnie z zasadami poufności, integralności, dostępności i autentyczności danych, przy zachowaniu możliwości wykazania ich przestrzegania, w szczególności ochronę fizyczną miejsc przetwarzania i przechowywania informacji oraz inne fizyczne i technologiczne sposoby zabezpieczenia dostępu do tych miejsc;
3) ustanowienie zasad gwarantujących bezpieczną pracę na odległość oraz pracę z wykorzystaniem sieci publicznych, w tym stosowanie zabezpieczeń antywirusowych oraz kontrolę poczty elektronicznej wewnątrz systemu informatycznego Jednostki;

4) dbanie o prawidłowe wykonywanie, przechowywanie oraz weryfikację pod względem kompletności i możliwości odtworzenia kopii zapasowych danych, wykorzystywanych w realizacji zadań publicznych nałożonych na Jednostkę;
5) stworzenie i testowanie procedur oraz wzorców działania na wypadek wystąpienia cyberzagrożenia, awarii lub wystąpienia incydentu bezpieczeństwa informacji;
6) ustanowienie zasad przyznawania, modyfikacji oraz cofania uprawnień dostępu do systemów i sieci informatycznych Pracownikom Jednostki lub innym uprawnionym osobom;
7) stworzenie zasad sprzyjających ustawicznemu podnoszeniu kwalifikacji oraz pogłębianiu wiedzy osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem:
   a) zasad cyberhigieny;
   b) rodzajów cyberzagrożeń;
   c) skutków naruszenia zasad bezpieczeństwa informacji;
   d) procedur na wypadek wystąpienia lub potencjalnego wystąpienia incydentu.

§8. OBOWIĄZEK ZAPOZNANIA SIĘ Z POLITYKĄ

Każda osoba, przed dopuszczeniem jej do przetwarzania informacji w Jednostce, zapoznaje się z Polityką oraz z zasadami bezpieczeństwa przewidzianymi w SZBI w zakresie dostosowanym do zakresu jej obowiązków i wykonywanych zadań i zobowiązuje się do ich przestrzegania. Fakt ten potwierdza poprzez podpisanie stosownego oświadczenia.

§9. DOSTĘPNOŚĆ

Polityka Bezpieczeństwa Informacji została opracowana i zatwierdzona przez Dyrektora Jednostki i jest dostępna do zapoznania się wszystkim zainteresowanym podmiotom na stronie internetowej Biuletynu Informacji Publicznej - https://zsebip.edu.bialystok.pl/.