Minister
Edukacji

DWST-WDiR.0915.1.2025.AJK

Warszawa, 14 lipca 2026 r.

Pan
Marek Charążka
Dyrektor Centrum Informatycznego Edukacji
al. J.Ch. Szucha 25
00-918 Warszawa
adres e-Doręczeń:
AE:PL-40428-45235-SVERI-22

WYSTĄPIENIE POKONTROLNE

Zgodnie z art. 47 ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej*[1] przekazuję niniejsze wystąpienie pokontrolne.

Na podstawie art. 6 ust. 3 pkt 1 ustawy z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej* oraz art. 25 ust. 1 pkt 3 lit. b ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[2], Ministerstwo Edukacji Narodowej[3] w terminie od 29 września 2025 r. do 30 stycznia 2026 r. przeprowadziło w Centrum Informatycznym Edukacji, z siedzibą przy al. J.Ch. Szucha 25, 00-918Warszawa, kontrolę w formie zdalnej pn. *Działanie i bezpieczeństwo wybranych systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych – w zakresie działania systemu informacji oświatowej*.

Celem kontroli było dokonanie oceny działania systemu teleinformatycznego pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych i wymiany informacji w postaci elektronicznej. Celem kontroli była także ocena działania systemu informacji oświatowej w zakresie zapewnienia działań usprawniających przed nowym rokiem szkolnym 2025/2026 oraz wdrożenia nowych funkcjonalności.
Kontrolą objęto okres od 1 stycznia 2025 r. do 30 września 2025 r., z uwzględnieniem działań wcześniejszych i późniejszych, jeżeli miały związek z przedmiotem kontroli.

Centrum Informatyczne Edukacji (dalej także: Centrum, CIE) jest państwową jednostką budżetową podległą Ministrowi Edukacji. W okresie objętym kontrolą Centrum Informatycznym Edukacji kierował Pan Marek Charążka[4].

[1] Dz.U. z 2026 r. poz. 158.
[2] Dz.U. z 2025 r. poz. 1703 z późn. zm.
[3] Kontrolę przeprowadzili pracownicy Ministerstwa:
1) Urszula Krauze, główny specjalista w Wydziale Danych i Rozwoju w Departamencie Współpracy z Samorządem Terytorialnym, na podstawie upoważnień nr 50/2025 z dnia 29 września 2025 r., nr 61/2025 z dnia 14 listopada 2025 r. i nr 63/2025 z dnia 30 grudnia 2025 r.;
2) Alicja Jakubiak-Kępińska, główny specjalista w Wydziale Kontroli w Departamencie Kontroli i Audytu, na podstawie upoważnień nr 51/2025 z dnia 29 września 2025 r., nr 62/2025 z dnia 14 listopada 2025 r. i nr 64/2025 z dnia 30 grudnia 2025 r.

[4] Funkcję Dyrektora CIE pełni od roku 2008.

Zgodnie ze Statutem Centrum Informatycznego Edukacji (dalej: Statut CIE) nadanym zarządzeniem Ministra Edukacji Narodowej z dnia 3 stycznia 2024 r. *w sprawie zmiany nazwy Informatycznego Centrum Edukacji i Nauki i nadania statutu Centrum Informatycznemu Edukacji*[5], przedmiot działalności CIE obejmuje:

1) obsługę informatyczną Ministerstwa Edukacji Narodowej (dalej także: MEN), w szczególności:
   a) projektowanie, programowanie, uruchamianie i utrzymywanie systemów informatycznych wspomagających zarządzanie i realizację zadań,
   b) zapewnienie rozwoju i rozbudowy utrzymywanych systemów informatycznych,
   c) zapewnienie bezpieczeństwa teleinformatycznego utrzymywanych systemów informatycznych,
   d) utrzymywanie i zapewnienie wymaganego standardu infrastruktury informatycznej,
   e) zarządzanie infrastrukturą teleinformatyczną, w tym gospodarowanie powierzonymi składnikami majątku,
   f) przechowywanie i udostępnianie danych, w tym zarchiwizowanych danych z obszaru oświaty i wychowania,
   g) wykonywanie kopii zapasowych administrowanych systemów i danych,
   h) zapewnienie dostępu do Internetu,
   i) obsługę systemów nagłośnienia i prezentacji w siedzibie Ministerstwa;
2) utrzymanie i rozwój systemu informacji oświatowej oraz przetwarzanie i udostępnianie zgromadzonych w nim danych, w uzgodnieniu z komórką organizacyjną Ministerstwa, do której zakresu działania należy prowadzenie spraw dotyczących wykonywania zadań wynikających z ustawy z dnia 15 kwietnia 2011 r. *o systemie informacji oświatowej*[6];
3) obsługę informatyczną zbiorów danych osobowych, których administratorem jest Minister, przechowywanych z wykorzystaniem infrastruktury serwerowej zarządzanej przez Centrum;
4) obsługę informatyczną jednostek podległych Ministrowi Edukacji w tym: Centralnej Komisji Egzaminacyjnej, Ośrodka Rozwoju Edukacji w Warszawie oraz Ośrodka Rozwoju Polskiej Edukacji za Granicą, na podstawie porozumienia;
5) obsługę informatyczną jednostek nadzorowanych przez Ministra Edukacji w tym: Instytutu Badań Edukacyjnych, Centrum Nauki Kopernik oraz Instytutu Rozwoju Języka Polskiego im. świętego Maksymiliana Marii Kolbego, na podstawie porozumienia;
6) wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, zgodnie z art. 21 ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa*[7].

Od lutego 2013 r. CIE jest certyfikowaną jednostką w zakresie ISO 27001[8].

Kontrolowany obszar regulują:

- ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[9] (dalej: ustawa o informatyzacji);
- rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w*

[5] Dz. Urz. ME poz. 1.
[6] Dz.U. z 2024 r. poz. 152 ze zm.
[7] Dz.U. z 2026 r. poz. 20.
[8] Certyfikat rejestracji nr 17008-ISMS-001PL ważny do 3 lutego 2028 r. potwierdzający zgodność zakresu Systemu Zarządzania Bezpieczeństwem Informacji Centrum Informatycznego Edukacji z wymaganiami ISO/IEC 27001:2022.
[9] Dz.U. z 2024 r. poz. 1557, ze zm.

postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[10] (dalej: rozporządzenie KRI);
- ustawa z 15 kwietnia 2011 r. *o systemie informacji oświatowej*;
- ustawa z dnia 14 grudnia 2016 r. – *Prawo oświatowe*[11].

Zgodnie z przepisami ustawy z dnia 15 kwietnia 2011 r. *o systemie informacji oświatowej*, przez system informacji oświatowej zapewnia się powszechny dostęp do informacji z zakresu oświaty (art. 1 ust. 2 ww. ustawy). SIO stanowią baza danych systemu informacji oświatowej (dalej: baza danych SIO) oraz system teleinformatyczny (art. 2 ww. ustawy).
System teleinformatyczny wykorzystywany w zakresie działania systemu informacji oświatowej (dalej także: system, SIO) dostępny jest pod adresem: https://sio.gov.pl/sio/login.
Ustawa *o systemie informacji oświatowej* określa organizację i zasady działania systemu informacji oświatowej służącego uzyskiwaniu danych niezbędnych do:

1) prowadzenia polityki oświatowej państwa na poziomie krajowym, regionalnym i lokalnym, w tym wspomagania zarządzania oświatą;
2) efektywnego funkcjonowania systemu finansowania zadań oświatowych na poziomie krajowym, regionalnym i lokalnym;
3) analizy efektywności wykorzystania środków publicznych przeznaczonych na finansowanie zadań oświatowych;
4) nadzorowania i koordynowania wykonywania nadzoru pedagogicznego na terenie kraju oraz podnoszenia jakości edukacji;
5) prowadzenia monitoringu karier absolwentów publicznych i niepublicznych szkół ponadpodstawowych.

Ww. ustawa zawiera m.in.: rodzaj i zakres danych gromadzonych w SIO (Rozdział 2); przekazywanie danych do bazy SIO, podmioty zobowiązane do przekazywania danych do bazy danych SIO (Rozdział 3); sposób i procedurę pozyskiwania danych dziedzinowych z bazy danych systemu informacji oświatowej, jak również danych ze zbiorów danych PESEL za pośrednictwem bazy danych systemu informacji oświatowej (Rozdział 4); dostęp do bazy danych SIO (Rozdział 5); regulacje dotyczące przechowywania danych w bazie danych (Rozdział 9); warunki organizacyjno-techniczne funkcjonowania systemu informacji oświatowej (Rozdział 10).

Użytkownikami SIO wskazanymi w załączniku nr 1 pn. *Lista usług głównych i aktywów-usług je wspierających* do Procedury Zarządzania Ryzykiem[12] (poz. 30 zestawienia) są „kierownicy i upoważnieni przez nich pracownicy:

1) publicznych i niepublicznych przedszkoli, szkół i placówek oraz innych jednostek organizacyjnych, o których mowa w art. 2 ustawy z dnia 14 grudnia 2016 r. - *Prawo oświatowe;*
2) innych jednostek wykonujących zadania z zakresu oświaty, tj.:
   a) jednostki samorządu terytorialnego,
   b) ministrowie prowadzący szkoły i placówki oświatowe,
   c) Centralna Komisja Egzaminacyjna,
   d) okręgowe komisje egzaminacyjne,
   e) jednostki organizacyjne, o których mowa w art. 1 ust. 1 pkt 2 ustawy z dnia 26 stycznia 1982 r. - *Karta Nauczyciela*[13],
   f) kuratoria oświaty,
   g) organy sprawujące nadzór pedagogiczny, o których mowa w art. 1 ust. 2 pkt 1 lit. e ustawy z dnia 26 stycznia 1982 r. – *Karta Nauczyciela*,

[10] Dz.U. z 2024 r. poz. 773.
[11] Dz.U. z 2025 r. poz. 1043.
[12] wersja 4.0 zatwierdzona przez Dyrektora CIE dnia 29.09.2023 r.
[13] Dz.U. z 2026 r. poz. 515.

h) specjalistyczne jednostki nadzoru, o których mowa w art. 53 ust. 1 i 2 ustawy z dnia 14 grudnia 2016 r. - *Prawo oświatowe*,
i) jednostki obsługujące, o których mowa w art. 10b ust. 1 ustawy z dnia 8 marca 1990 r. *o samorządzie gminnym*[14], art. 6b ust. 1 ustawy z dnia 5 czerwca 1998 r. *o samorządzie powiatowym*[15] lub art. 8d ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa[16], które obejmują wspólną obsługą szkoły i placówki oświatowe założone i prowadzone przez jednostki samorządu terytorialnego,
j) izby rzemieślnicze".

Wsparcie dla użytkowników SIO w postaci instrukcji technicznych, instrukcji merytorycznych i filmów instruktażowych znajduje się na stronie https://pomoc.sio.gov.pl oraz na stronie CIE pod adresem: https://cie.gov.pl/wsparcie-dla-uzytkownikow-sio/.

Ocena ogólna kontrolowanej działalności.

Na podstawie wyników kontroli pozytywnie oceniono obszar objęty kontrolą.

I. Podejmowanie przez CIE działań usprawniających system informacji oświatowej przed rokiem szkolnym 2025/2026 oraz wdrożenie w SIO nowych funkcjonalności.

Dostawcą usług dla Centrum Informatycznego Edukacji w zakresie obsługi SIO od 1 kwietnia 2024 r. jest firma Softiq Sp. z o.o. W dniu 18 marca 2024 r. została zawarta umowa nr CIE-11/2024 pomiędzy CIE (będący Zamawiającym) a firmą zewnętrzną (będący Wykonawcą), której przedmiotem jest świadczenie usługi utrzymania systemu w trybie produkcyjnym, w tym usługi programistyczne na potrzeby utrzymania w ruchu Systemu Informacji Oświatowej i usługi administracji systemem, oraz prace rozwojowe w trakcie trwania umowy. Zgodnie z § 1 umowy Wykonawca zobowiązał się do wykonywania usług na zasadach i warunkach ustalonych w umowie, której integralną część stanowią nw. załączniki:
- załącznik nr 1: formularz oferty,
- załącznik nr 2: Opis Przedmiotu Zamówienia (OPZ)[17],
- załącznik nr 3: wzór protokołu odbioru prac rozwojowych w zamówieniu podstawowym,
- załącznik nr 4: wzór protokołu odbioru opcjonalnych prac rozwojowych,
- załącznik nr 5: wór umowy powierzenia danych osobowych.

Umowa została zawarta na okres od 1 kwietnia 2024 r. do 31.03.2027 r.

Na początku roku szkolnego 2024/2025 odnotowano zgłoszenia o nieprawidłowościach w zapewnieniu ciągłości działania systemu SIO, które głównie dotyczyły:
- wolniejszego działania systemu,
- przerw w dostępie do systemu,
- problemów technicznych uniemożliwiających użytkownikom wprowadzanie danych do bazy, takich jak: brak bocznego paska narzędzi, błędne wyświetlanie etykiet, niepoprawne działanie filtrów, brak możliwości wysłania formularza zgłoszeniowego po zalogowaniu do strefy pracownika SIO.

[14] Dz.U. z 2025 r. poz. 1153, poz. 1436, z 2026 r. poz. 252.
[15] Dz.U. z 2025 r. poz. 1684, z 2026 r. poz. 252.
[16] Dz.U. z 2025 r. poz. 581, poz. 1535, z 2026 r. poz. 252.
[17] Opis Przedmiotu Zamówienia (OPZ) stanowiący załącznik nr 2 do Specyfikacji Warunków Zamówienia (SWZ) w postępowaniu o udzielenie zamówienia publicznego pn. „Świadczenie usługi utrzymania w ruchu w trybie produkcyjnym Systemu Informacji Oświatowej", numer referencyjny: ZA.230.4.2023 przeprowadzonego w trybie przetargu nieograniczonego.

CIE otrzymało we wrześniu 2024 r. od użytkowników SIO zgłoszenia dotyczące braku możliwości pracy w systemie, spowodowanej jego dużym spowolnieniem. W związku ze zgłaszanymi przez użytkowników SIO nieprawidłowościami w zapewnieniu ciągłości działania systemu, CIE zleciło – zgodnie z zapisami OPZ – firmie Softiq Sp. z o.o. usunięcie wskazanych błędów i poprawę jakości wykonywania przedmiotu Umowy. Podczas kontroli przekazano informacje dotyczące zgłaszanych problemów z działaniem systemu, które to problemy znacząco utrudniały, a w wielu przypadkach uniemożliwiały użytkownikom systemu pracę w programie SIO[18].

Z uwagi na wolne działanie systemu użytkownicy nie byli w stanie realizować obowiązków nałożonych na nich ustawą z dnia 15 kwietnia 2011 r. *o systemie informacji oświatowej*, tj. przekazywać w ustawowym terminie[19] danych do systemu. Dzianie systemu uniemożliwiające użytkownikom wprowadzanie danych pierwotnie zostało zakwalifikowane przez CIE jako błąd krytyczny[20]. Zgodnie z definicją Zgłoszenia o Poziomie Krytycznym określoną w OPZ jest to „zgłoszenie błędu objawiającego się nieprawidłowym działaniem Systemu, powodującym:

1) niedostępność Systemu lub jego poszczególnych funkcji, lub
2) nieprawidłowość działaniu Systemu uniemożliwiającą realizację procesów biznesowych lub realizację kluczowej funkcjonalności przez System, lub
3) generowanie nieprawidłowych danych".

W odpowiedzi Firma Softiq Sp. z o.o. argumentowała[21] zmniejszoną wydajność systemu na początku roku szkolnego 2024/2025 dużym obciążeniem pracy użytkowników, przyjętą wówczas architekturą systemu i zastosowanymi w całym systemie rozwiązaniami implementacyjnymi, jak również wskazywała na możliwości wprowadzania zmian/poprawek w systemie jedynie w trakcie przerw serwisowych (brak możliwości wprowadzania zmian bez zatrzymania Systemu). Wykonawca przedstawił CIE dokumenty[22] wykazujące, że powyższe problemy z funkcjonowaniem systemu nie stanowiły przesłanek, by zakwalifikować zgłoszone nieprawidłowości jako błąd krytyczny. Wykonawca wskazał zmiany[23] jakie wdrożył w dniach 3-25 września, obejmujące m.in.:

- optymalizację działania aplikacji SIO,
- konfigurację poszczególnych elementów infrastruktury: bazy danych, serwerów aplikacyjnych, kolejek,
- optymalizację zapytań do bazy danych.

Po dokonaniu przez CIE analizy posiadanej dokumentacji oraz danych systemowych z września 2024 r., CIE zakwalifikowało zaistniałą awarię jako błąd średni. Zgodnie z definicją Zgłoszenia o Poziomie Średnim, określoną w OPZ jest to „zgłoszenie błędu objawiającego się nieprawidłowym działaniem Systemu, powodującym:

1) ograniczenie w sposób istotny możliwość korzystania z Systemu lub jego poszczególnych funkcji, lub
2) istotne utrudnienia w korzystaniu z funkcji Systemu, lub

---

[18] Dokument pn. „Lista zadań zgłoszonych w jira-srv do programistów".

[19] Zgodnie z art. 30 ust. 1 ustawy z dnia 15 kwietnia 2011 r. *o systemie informacji oświatowej* podmiot zobowiązany do przekazywania danych do zbioru danych szkoły lub placówki oświatowej, zbioru danych jednostki, zbioru danych nauczyciela i zbioru danych ucznia przekazuje dane do bazy danych SIO, w terminie 7 dni od dnia, w którym nastąpiła zmiana w stanie faktycznym (…).

[20] Pismo CIE z 17 października 2024 r. do firmy Softiq Sp. z o.o.

[21] Pismo firmy Softiq Sp. z o.o. z 24 października 2024 r.

[22] Dokumenty stanowiące kolejno załączniki nr 2 i 3 do pisma firmy Softiq Sp. z o.o. z 24 października 2024 r. pn. *Statystyki przypisań uczniów do oddziałów w dniach 02-30.09* oraz *Analiza problemów wydajnościowych SIO 4 października 2024 r.*

[23] Szczegółowy zakres zmian raportowany codziennie został przedstawiony w załączniku do pisma firmy Softiq Sp. z o.o. z 24 października 2024 r. – załącznik nr 1 pn. „Wrzesień 2024 - zmiany związane z wdrożeniem/wydajnością".

3) możliwość generowania przez System nieprawidłowych danych".

CIE zobowiązało[24] Wykonawcę do przedstawienia raportu z analizy przyczyn wystąpienia błędów systemu na początku roku szkolnego 2024/2025, w celu zapewnienia sprawnego i niezakłóconego uzupełniania danych oświatowych w systemie przez użytkowników w przyszłości. W odpowiedzi[25] firma Softiq Sp. z o.o. przekazała opis zrealizowanych czynności, takich jak: przeprowadzenie diagnostyki systemu, wskazującej na problemy wydajnościowe SIO[26]; przeprowadzenie testów wydajnościowych systemu[27], które wykazywały problemy ze stabilnością przy aktywnym module monitorującym; przeprowadzenie testów operacji grupowych[28], porównujących pracę na starej synchronicznej architekturze z nową asynchroniczną architekturą; opracowanie planu poprawy wydajności systemu[29], zawierającego ramowy harmonogram prac oraz listę rekomendowanych działań optymalizacyjnych oraz przeprowadzenie prac konfiguracyjnych, optymalizacyjnych i programistycznych[30].

Działania zlecone przez CIE oraz działania podjęte przez firmę Sotfiq Sp. z o.o. po wrześniu 2024 r. zapewniły na początku roku szkolnego 2025/2026 ciągłość działania SIO (we wrześniu 2025 r. nie stwierdzono niestabilności systemu) – przeprowadzono testy wydajnościowe[31] dla 15 tys. użytkowników mające na celu sprawdzenie stabilności środowiska. Dokonano również porównania[32] przeprowadzonych w odstępnie 5 miesięcy testów wydajnościowych, których wyniki wskazują na wzrost liczby obsłużonych żądań i średniej przepustowości żądań na sekundę, przy jednoczesnym spadku średniego czasu odpowiedzi oraz zmniejszeniu się liczby błędów.
Z wyjaśnień CIE wynika[33], że działania podjęte przez firmę Softiq Sp. z o.o. wskazują, że wprowadzane zmiany przyniosły zakładane efekty a problemy z funkcjonowaniem systemu we wrześniu 2024 r. mogły być spowodowane m.in. ograniczeniami wydajnościowymi systemu na poziomie aplikacyjnym i na poziomie infrastruktury.

CIE wdrożyło nw. nowe funkcjonalności SIO, wpływające na sposób wykazywania danych od roku szkolnego 2025/2026. Wdrożone funkcjonalności dotyczyły:
1) możliwości tworzenia tzw. oddziałów roboczych od roku szkolnego 2025/2026, w sierpniu na nowy rok szkolny, bazując na oddziale z bieżącego roku szkolnego;

[24] Pismo CIE z 7 marca 2025 r., znak: ZPiA.471.1.2024.
[25] Pismo firmy Softiq Sp. z o.o. z 21 maja 2025 r.
[26] Załącznik nr 5 pn. „Analiza problemów wydajnościowych SIO v3.1 2024-10-04" (stan na 19.05.2025 r.) oraz załącznik nr 6 pn. „Diagnoza problemów wydajnościowych Systemu Informacji Oświatowej" do pisma firmy Softiq Sp. z o.o. z 21 maja 2025 r.
[27] Załącznik nr 4 pn. „Wyłączenie AppDynamics na serwerach webowych 2024-09-24" oraz załącznik nr 7 pn. „Raport AppDynamics" do pisma firmy Softiq Sp. z o.o. z 21 maja 2025 r.
[28] Załącznik nr 8 pn. „Raport testów operacji grupowych" do pisma firmy Softiq Sp. z o.o. z 21 maja 2025 r.
[29] Załącznik nr 9 pn. „Plan poprawy wydajności 2025-05-19" do pisma firmy Softiq Sp. z o.o. z 21 maja 2025 r.
[30] Załącznik nr 10 pn. „Raport z optymalizacji bazy danych MySQL" do pisma firmy Softiq Sp. z o.o. z 21 maja 2025 r.
[31] Został opracowany dokument pn. „Raport z testów wydajnościowych dla 15k użytkowników" stanowiący załącznik nr 1 do pisma firmy Softiq Sp. z o.o. z 18 sierpnia 2025 r.
[32] Testy porównawcze wykonano przy ruchu generowanym przez 5 000 wirtualnych użytkowników, z uwagi na przeprowadzanie wcześniejszych testów na takiej liczbie użytkowników. Przedstawiony został dokument pn. „Porównanie wyników z 03/2025" stanowiący załącznik nr 2 do pisma firmy Softiq Sp. z o.o. z 18 sierpnia 2025 r.
[33] Pismo CIE z 15 października 2025 r.; znak: ZPiA.471.1.2024.

oddziały robocze po 1 września będą automatycznie przekształcone w bieżące oddziały na kolejny rok szkolny[34];

2) aktualizacji słowników w zakresie zawodów[35] w związku ze zmianami w klasyfikacji zawodów szkolnictwa branżowego, obejmującymi wprowadzenie nowych zawodów oraz modyfikację podstaw programowych (obwieszczenie Ministra Edukacji z dnia 19 marca 2024 r. *w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Edukacji Narodowej w sprawie ogólnych celów i zadań kształcenia w zawodach szkolnictwa branżowego oraz klasyfikacji zawodów szkolnictwa branżowego*[36] – załącznik nr 2 do rozporządzenia);
3) możliwości rejestracji miejsca realizacji indywidualnego nauczania dla uczniów szkoły i miejsca realizacji zajęć indywidualnego obowiązkowego rocznego przygotowania przedszkolnego dla oddziałów przedszkolnych[37] (rozporządzenie Ministra Edukacji z dnia 19 listopada 2024 r. *zmieniające rozporządzenie w sprawie indywidualnego obowiązkowego rocznego przygotowania przedszkolnego dzieci i indywidualnego nauczania dzieci i młodzieży*[38]);
4) możliwości rejestracji informacji o korzystaniu z nauki języka i kultury kraju pochodzenia wyłącznie dla uczniów cudzoziemców[39] o których mowa w art. 165 ust. 15 ustawy – *Prawo oświatowe;*
5) obowiązku rejestracji danych dotyczących kraju pochodzenia i statusu przy identyfikacyjnych uczniów bez numeru PESEL i cudzoziemców[40] (art. 11 ustawy z dnia 15 kwietnia 2011 r. *o systemie informacji oświatowej)*;
6) możliwości gromadzenia danych o liczbie uczniów, z podaniem ich płci i klasy, uczestniczących w zajęciach edukacja zdrowotna[41] w związku z wprowadzeniem w szkołach od 1 września 2025 r. przedmiotu „edukacja zdrowotna" (rozporządzenie Ministra Edukacji z dnia 6 marca 2025 r. *zmieniające rozporządzenie w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla*

---

[34] Instrukcja tworzenia w SIO oddziałów roboczych na nowy rok szkolny dostępna jest pod adresem: https://pomoc.sio.gov.pl/tech_instruction/oddzialy-robocze-na-nowy-rok-szkolny/
Zgodnie z oświadczeniem CIE z 1.12.2025 r. (wiadomość e-mail) możliwości tworzenia oddziałów roboczych została wgrana na produkcję 18.08.2025 r.

[35] Zgodnie z oświadczeniem CIE z 1.12.2025 r. (wiadomość e-mail) aktualizacja słowników w zakresie zawodów została wgrana na produkcję 18.08.2025 r.

[36] Dz.U. z 2024 r. poz. 611.

[37] Instrukcja wprowadzania w SIO miejsca prowadzenia zajęć nauczania indywidualnego dostępna jest pod adresem: https://pomoc.sio.gov.pl/tech_instruction/rejestracja-13/
Zgodnie z oświadczeniem CIE z 1.12.2025 r. (wiadomość e-mail) możliwości wykazania informacji o miejscu realizacji nauczania indywidualnego została wgrana na produkcję 3.09.2025 r.

[38] Dz.U. z 2024 r. poz. 1714.

[39] Instrukcja wprowadzania do SIO pozostałych danych dziedzinowych takich jak „korzystanie z nauki języka i kultury kraju pochodzenia" dostępna jest pod adresem: https://pomoc.sio.gov.pl/tech_instruction/rejestracja-13/

[40] Instrukcja wprowadzania danych do SIO o uczniu nieposiadającego numeru PESEL i niebędącego obywatelem polskim jest dostępna pod adresem: https://pomoc.sio.gov.pl/instruction/uczniowie-dane-identyfikacyjne/

[41] Instrukcja wprowadzania w SIO informacji dotyczących edukacji zdrowotnej dostępna jest pod adresem: https://pomoc.sio.gov.pl/tech_instruction/edukacja-zdrowotna-rejestracja/
Zgodnie z oświadczeniem CIE z 1.12.2025 r. (wiadomość e-mail) funkcjonalność została wgrana na produkcję 3.09.2025 r.

szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej [42]);

7) możliwości dodania oddziału o profilu mundurowym w liceach i technikach[43] w związku z wprowadzeniem możliwości utworzenia oddziału o profilu mundurowym przez organy prowadzące publiczne i niepubliczne szkoły ponadpodstawowe, po uzyskaniu zezwolenia udzielonego przez Ministra Spraw Wewnętrznych i Administracji (art. 28aa ustawy - *Prawo oświatowe);*
8) możliwości dodania rejestracji legitymacji szkolnej[44] w celu umożliwienia wydania mLegitymacji szkolnej z wykorzystaniem aplikacji mObywatel (art. 66e ustawy *o systemie informacji oświatowej).*

Wskazane wyżej funkcjonalności systemu, wpływające na sposób wykazywania danych w SIO zostały wdrożone, umożliwiając użytkownikom systemu korzystanie z nich od początku roku szkolnego 2025/2026.

Z przedstawionej w toku kontroli dokumentacji wynika, że czynności zlecone przez CIE firmie Softiq Sp. z o.o. przyczyniły się do poprawy funkcjonowania SIO po wrześniu 2024 r. pod względem zapewnienia ciągłości i stabilności działania systemu na początku roku szkolnego 2025/2026.

Ocena cząstkowa badanego obszaru: pozytywna.

II. Zgodność z minimalnymi wymaganiami dla systemów teleinformatycznych i wymiany informacji w postaci elektronicznej.

1. System zarządzania bezpieczeństwem informacji.

Wymogi dotyczące systemu zarządzania bezpieczeństwem informacji dla podmiotów realizujących zadania publiczne zostały określone w § 19 i 20 rozporządzenia KRI.

Zgodnie z § 19 ww. rozporządzenia KRI:

ust. 1. *Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.*

ust. 2. *Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: (…);*
działania określono w pkt 1-14.

ust. 3. *Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:*
   1) *PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń;*
   2) *PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem.*

---

[42] Dz.U. z 2025 r. poz. 378.

[43] Instrukcja określania w SIO specyfiki dodatkowej oddziału, jak np. o profilu mundurowym dostępna jest pod adresem: https://pomoc.sio.gov.pl/instruction/oddzialy-podstawowe/
Zgodnie z oświadczeniem CIE z 1.12.2025 r. (wiadomość e-mail) możliwość rejestracji oddziału o profilu mundurowym w liceach i technikach została wgrana na produkcję 18.08.2025 r.

[44] Instrukcja rejestracji legitymacji szkolnych celem zarejestrowania mLegitymacji dostępna jest pod adresem: https://pomoc.sio.gov.pl/tech_instruction/rejestracja-legitymacji-szkolnych/
Zgodnie z oświadczeniem CIE z 1.12.2025 r. (wiadomość e-mail) możliwość rejestracji legitymacji szkolnej została wgrana na produkcję 16.09.2025 r.

CIE jest certyfikowaną jednostką w zakresie ISO 27001 od lutego 2013 r.; posiada certyfikat rejestracji nr 17008-ISMS-001PL wydany 2 maja 2025 r., ważny do 3 lutego 2028 r., zatwierdzony przez jednostkę akredytowaną Alcumus ISOQAR, który zaświadcza zgodność Systemu Zarządzania Bezpieczeństwem Informacji Centrum Informatycznego Edukacji z wymaganiami ISO/IEC 27001:2022.

Wobec powyższego, zgodnie z ww. § 19 ust. 3 rozporządzenia KRI wymagania określone w § 19 ust. 1 i 2 KRI uznano za spełnione.

System Zarządzania Bezpieczeństwem Informacji w CIE (dalej: SZBI) został ustanowiony decyzją nr 7 z dnia 27.09.2024 r. Dyrektora Centrum Informatycznego Edukacji *w sprawie wdrożenia w Centrum Informatycznym Edukacji Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z normą PN-ISO/IEC 27001:2022*.

Zgodnie z ww. decyzją na dokumentację SZBI w CIE składają się: Polityka Bezpieczeństwa Informacji (PBI); Polityka Ochrony Danych Osobowych (PODO); Polityka Administrowania Systemami Informatycznymi (PASI); Polityka Bezpieczeństwa Osobowego (PBO); Polityka Kontroli Dostępu (PKD); Polityka Ciągłości Działania (PCD); Procedura Zarządzania Aktywami (PZA); Polityka Wytwarzania Oprogramowania (PWO); Polityka Komunikacji (PK); Procedura Zarządzania SZBI (PZSZBI); Polityka Dostępu do Pomieszczeń (PDP); - Procedura Zarządzania Hasłami (PZH); Procedura Zarządzania Incydentem Ciągłości Działania (PZICD); Procedura Zarządzania Ryzykiem (PZR); Procedura Oznaczania Informacji (POI); Procedura Przekazywania Informacji (PPI); Procedura Nadzoru nad Dokumentami i Zapisami (PDZ); Procedura Audytów (PA); Procedura Działań Korygujących i Zapobiegawczych (PDNZ); Procedura Rekrutacji i Derekrutacji (PRD); Procedura Inwentaryzacji Aktywów (PIA); Procedura Przydzielania i Przekazywania Mienia (PPPM); Procedura Postępowania Dyscyplinarnego (PPD); Procedura Weryfikacji Kandydata (PWK); Procedura Łańcucha Dostaw (PŁD); Procedura Kontaktu z dostawcami, klientami i innymi stronami zewnętrznymi (PKDKS); Procedura Zarządzania Zmianą (PZZ); Procedura Zarządzania Bezpieczeństwem IT (PZBIT); Procedura Zarządzania Dostępem do Sejfów (PZDS); Procedura Zarządzania Testami w Systemach Informatycznych (PZT w SI); Procedura Otwarcia Pomieszczenia w Trybie Awaryjnym (POPTA); Procedura Postępowania w Przypadku Awarii SKD (PPPA); Procedura Pobierania Kluczy (PPK); Procedura Postępowania z Pomieszczeniami Stref IV (PPPS); Procedura Postępowania z Nośnikami (PPN); Procedura Tworzenia Kopii Zapasowych (PTKZ); Procedura Zarządzania Incydentami (PZIBI); Procedura Zarządzania Uprawnieniami (PZU); Kalendarz Okien Serwisowych (KOS); Procedura Zgłaszania Incydentów (PZI).

W § 3 ww. decyzji zawarto, że opiekę nad prawidłowym funkcjonowaniem systemu SZBI sprawuje wyznaczony pracownik ZAiBI[45], który pełni funkcję Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji (ust. 1); szczegółowe zadania pracownika odpowiedzialnego za opiekę nad prawidłowym funkcjonowaniem SZBI określa dokumentacja SZBI i jego zakres obowiązków (ust. 2).

W zakresie objętym kontrolą przedstawiono następujące dokumenty:

1. *Polityka Bezpieczeństwa Informacji* (wersja 6.1 zatwierdzona przez Dyrektora CIE dnia 14.02.2024 r. oraz wersja 6.2 zatwierdzona przez Dyrektora CIE dnia 18.07.2025 r.) wraz z załącznikami:
   - załącznik nr 1 – Słownik Terminów i Skrótów (wersja 3.0 z dnia 29.12.2023 r.);
   - załącznik nr 2 – Hierarchia Dokumentacji (wersja 3.4 z dnia 29.12.2023 r.);

[45] ZAiBI – Zakład Administracyjny i Bezpieczeństwa Informacji; na podstawie *Regulaminu organizacyjnego Centrum Informatycznego Edukacji* zatwierdzonego 5.01.2024 r. przez Dyrektora Generalnego MEN (Rozdział I. Zasady organizacji i zarządzania, ust. 3. Struktura organizacyjna Centrum pkt 4).

- załącznik nr 3 – Ogólne zasady Zarządzania Bezpieczeństwem Informacji (wersja 4.0 z dnia 29.12.2023 r.);
- załącznik nr 4 – Interesariusze CIE i ich wymagania w zakresie SZBI (wersja 1.2 z dnia 29.12.2023 r.);
- załącznik nr 5 – Role i Odpowiedzialności w SZBI (wersja 3.4 z dnia 29.12.2023 r.);
- załącznik nr 6 – Uwarunkowania Prawne (wersja 3.5 z dnia 23.02.2024 r.).

PBI określa: ogólne zasady stosowania zabezpieczeń, w tym organizowania szkoleń mających na celu zwiększanie świadomości użytkowników w zakresie bezpieczeństwa informacji, naruszenia zasad zarządzania bezpieczeństwem informacji, postępowanie w przypadku uzasadnionego podejrzenia naruszenia bezpieczeństwa informacji, działania podejmowane w przypadku naruszenia bezpieczeństwa informacji; zarządzanie systemami i sieciami, w tym procedury eksploatacyjne oraz zakresy odpowiedzialności, ochronę przed szkodliwym oprogramowaniem, korzystanie z Intranetu, Internetu oraz z poczty elektronicznej; kontrolę dostępu do systemu, w tym zakres odpowiedzialności użytkowników i hasła dostępu; bezpieczeństwo urządzeń mobilnych, w tym służbowe telefony komórkowe i tablety oraz służbowe komputery przenośne.

W załączniku nr 6 do PBI – Uwarunkowania Prawne zostały wymienione wymagania wynikające z Normy ISO/IEC 27001:2022 i innych regulacji. Załącznik jest udostępniony w przestrzeni Sharepoint. Dostęp do ww. dokumentu posiada każdy z pracowników CIE.

2. *Procedura Zarządzania Aktywami* (zatwierdzona przez Dyrektora CIE dnia 4.10.2023 r.). Celem tej procedury jest określenie zasad obejmujących m.in.: sposoby zabezpieczenia aktywów informacyjnych, ich ochrony przed niepożądanym działaniem środowiska, oraz zapobiegania nieautoryzowanemu dostępowi do zasobów lub ich uszkodzeniu skutkującym zakłóceniem pracy CIE; przyznawanie i przekazywanie pracownikom CIE sprzętu teleinformatycznego, oprogramowania oraz innego wyposażenia niezbędnego do wykonywania obowiązków służbowych/zadań.
3. *Procedura Inwentaryzacji Aktywów* (wersja 1.1 zatwierdzona przez Pełnomocnika ds. SZBI dnia 18.07.2024 r. oraz wersja 1.2 zatwierdzona przez Pełnomocnika ds. SZBI dnia 15.05.2025 r.) wraz z załącznikami:
   - załącznik nr 1 – Formularz inwentaryzacji aktywów (wersja 2.2 z dnia 27.08.2021 r.);
   - załącznik nr 2 – Kryteria ważności aktywów (wersja 2.2 z dnia 27.08.2021 r.);
   - załącznik nr 3 – Zasady postępowania z aktywami informacyjnymi (wersja 2.3 z dnia 18.07.2024 r.).
4. *Procedura Zarządzania Ryzykiem* (wersja 4.0 zatwierdzona przez Dyrektora CIE dnia 29.09.2023 r. oraz wersja 5.0 zatwierdzona przez Dyrektora CIE dnia 09.01.2025 r.) wraz z załącznikami:
   - załącznik nr 1 – Lista usług głównych i aktywów-usług je wspierających;
   - załącznik nr 2 – Szablon Analizy Ryzyka dla usług głównych i aktywów usług je wspierających;
   - załącznik nr 3 - Szablon Analizy Ryzyka dla aktywów informacyjnych;
   - załącznik nr 4 – Plany Mitygacji;
   - załącznik nr 5 – Pan minimalizacji ryzyka;
   - załącznik nr 6 – Raport półroczny dla usług głównych i aktywów/usług je wspierających;
   - załącznik nr 7 – Raport roczny dla aktywów informacyjnych;
   - załącznik nr 8 - Struktura Szablonu Analizy Ryzyka;
   - załącznik nr 9 – Rejestr Ryzyk.

   Zgodnie z zakresem stosowania *Procedury Zarządzania Ryzykiem* określonym w pkt 2, ww. procedurę stosuje się „do określenia poziomu ryzyka dla aktywów informacyjnych.

Analizę ryzyka przeprowadza się raz do roku dla wszystkich aktywów głównych oraz aktywów wspierających".

5. *Polityka Administrowania Systemami Informatycznymi* (wersja 5.0 zatwierdzona przez Dyrektora CIE dnia 13.12.2023 r.).
   Celem ww. polityki, wskazanym w cz. 1, jest „opisanie przebiegu najważniejszych czynności zapewniających użytkownikom odpowiednią jakość dostępu do systemów informatycznych poprzez udostępnienie usług oraz stanowisk pracy oraz wymaganą funkcjonalność przy równoczesnym zapewnieniu spełnienia wymogów bezpieczeństwa informacji".
   Dokument zawiera opis postępowania w zakresie: zapewnienia bezpieczeństwa komputerów osobistych (w tym przenośnych), serwerów, serwerów wirtualnych i innych urządzeń/systemów, sieci komputerowych, okablowania i sprzętu, informacji przy korzystaniu z usług w chmurze; wydzielenia pomieszczenia bezpieczeństwa systemu; wykonywania kopii zapasowych; przeglądania danych w systemach (alertów wynikających z logów); monitorowania podatności technicznych urządzeń, systemów oraz wykorzystania zasobów sprzętowych; prowadzenia Dziennika Administratora Technicznego.
6. *Polityka Tematyczna Przetwarzania Logów* (wersja 1.0 zatwierdzona przez Dyrektora CIE dnia 23.02.2024 r.).
   Zgodnie z cz. 1 ww. polityki, celem polityki jest „zapewnienie rozliczalności i zgodności z wymaganiami KRI w systemach teleinformatycznych poprzez wiarygodne dokumentowanie zapisów dzienników systemowych (logach) w postaci elektronicznej".
7. *Polityka Wytwarzania Oprogramowania* (wersja 2.0 zatwierdzona przez Dyrektora CIE dnia 9.01.2026).
   Celem ww. polityki, wskazanym w cz. 1, jest „określenie wytycznych dotyczących tworzenia, rozwijania i utrzymania aplikacji, w szczególności z wykorzystaniem technologii takich jak PHP, JavaScript, HTML oraz CSS. Polityka ma na celu zapewnienie odpowiedniej jakości, bezpieczeństwa i spójności kodu źródłowego oraz wspieranie dobrych praktyk inżynierii oprogramowania w organizacji. Jej wdrożenie pozwala na tworzenie rozwiązań spełniających wymagania funkcjonalne, techniczne i zgodnych z obowiązującymi standardami jakości". Zgodnie z zakresem określonym w ww. polityce, dokument ten „ma zastosowanie do wszystkich działań związanych z wytwarzaniem, rozwijaniem oraz wprowadzaniem zmian w systemach informatycznych wykorzystywanych w Centrum. Obejmuje zarówno nowe projekty, jak i modyfikacje istniejących systemów, niezależnie od etapu cyklu życia oprogramowania".

Zgodnie z § 19 ust. 4 rozporządzenia KRI – *niezależnie od zapewnienia przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.*

Zastępca Dyrektora CIE w odpowiedzi na pismo MEN[46] o wskazanie dodatkowych zabezpieczeń jakie zostały przez CIE ustanowione, niezależnie od zapewnienia warunków umożliwiających realizację i egzekwowanie działań, o których mowa w § 19 ust. 2 ww. rozporządzenia KRI, wskazał[47]: „Dodatkowo poziom bezpieczeństwa systemu SIO jest wzmacniany poprzez zastosowanie wyspecjalizowanych narzędzi technicznych, w szczególności:

[46] Pismo MEN z 27.01.2026 r., znak: DWST-WDiR.0915.1.2025.AJK2.
[47] Pismo CIE z 3.02.2026 r., znak: ZPiA.061.1.2025.

a) systemu klasy PAM (Privileged Access Management) – zapewniającego kontrolę dostępu do kont uprzywilejowanych oraz rejestrację i nagrywanie sesji administracyjnych,
b) systemu klasy DLP (Data Loss Prevention) – monitorującego przepływ danych i zapobiegającego ich nieuprawnionemu ujawnieniu lub wyciekowi,
c) systemu Dynatrace – realizującego skanowanie aplikacji pod kątem podatności bezpieczeństwa,
d) systemu Zabbix – monitorującego infrastrukturę techniczną w zakresie dostępności, wykrywającego awarie systemów oraz elementów sprzętowych.

Zastosowane środki stanowią uzupełnienie standardowych mechanizmów bezpieczeństwa i są adekwatne do zidentyfikowanych zagrożeń oraz poziomu ryzyka związanego z przetwarzaniem danych w systemie SIO".

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 20 rozporządzenia KRI:

ust. 1. *Rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach).*

ust. 2. *W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do:*
   1) systemu z uprawnieniami administracyjnymi;
   2) konfiguracji systemu, w tym konfiguracji zabezpieczeń;
   3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.

ust. 3. *Poza informacjami wymienionymi w ust. 2 mogą być odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci:*
   1) działań użytkowników nieposiadających uprawnień administracyjnych,
   2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu,
   3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny
   - w zakresie wynikającym z analizy ryzyka.

ust. 4. *Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.*

Zgodnie z opracowaną *Polityką Administrowania Systemami Informatycznymi*[48] „każdy administrator techniczny jest zobowiązany do prowadzenia Dziennika Administratora technicznego w formie elektronicznej w dedykowanej przestrzeni Confluence. (…) Administrator techniczny jest zobowiązany do odnotowywania w „Dzienniku AT" wszelkich dokonywanych istotnych zmian w administrowanym systemie mających lub mogących mieć wpływ na działanie systemu (zmiana konfiguracji, aktualizacja, modyfikacja kont, modyfikacja sprzętu, obsługa incydentów)".

W załączniku nr 5 (Role i Odpowiedzialności w SZBI) do PBI określone zostały role, zakres odpowiedzialności oraz struktura organizacyjna w SZBI.

Celem opracowanej *Polityki Tematycznej Przetwarzania Logów*[49] jest zapewnienie rozliczalności i zgodności z wymaganiami KRI w systemach teleinformatycznych poprzez dokumentowanie zapisów dzienników systemowych (logach) w postaci elektronicznej. Zgodnie z zapisami ww. Polityki:

[48] Symbol dokumentu: ICEiN/SZBI/PASI, data wydania dokumentu: 13.12.2023 r., wersja 5.0.
[49] Symbol dokumentu: CIE/SZBI/PASI/PPL, data wydania dokumentu: 23.02.2024 r., wersja 1.0.

- „informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres dwóch lat, chyba że pisemne ustalenie z Właścicielem Aktywa danego systemu lub przepisy odrębne stanowią inaczej" (4.1.3.);
- „logi przechowywane są przez okres minimum 2 lata, chyba że pisemne ustalenie z Właścicielem Aktywa stanowi inaczej. Dostęp do serwera logów jest ograniczony do osób dopuszczonych przez ABT" (4.3.1.).

Obowiązek przeglądania danych w logach systemów oraz usług został także wskazany w Opisie Przedmiotu Zamówienia stanowiącym załącznik nr 2 do umowy nr CIE-11/2024, gdzie zawarto, że „Poprzez utrzymanie w trybie produkcyjnym rozumie się dokonywanie wszelkich czynności technicznych w ramach świadczonej usługi, w szczególności przeglądanie danych w logach systemów oraz usług" (rozdział 2 pkt 1.3. lit. v OPZ).

W badanym zakresie nie stwierdzono nieprawidłowości.

Ocena cząstkowa badanego obszaru: pozytywna.

2. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.

Przepisy dotyczące wymiany informacji w postaci elektronicznej zostały określone w art. 16 ustawy *o informatyzacji* oraz w § 5 i § 15-18 rozporządzenia KRI.

- Zgodnie z art. 16 ustawy o informatyzacji:

ust. 1. *Podmiot publiczny, który organizuje przetwarzanie danych w systemie teleinformatycznym, jest obowiązany zapewnić możliwość przekazywania danych przez wymianę dokumentów elektronicznych związanych z załatwianiem spraw należących do jego zakresu działania. Do przekazywania danych podmiot ten wykorzystuje informatyczne nośniki danych lub środki komunikacji elektronicznej.*

ust. 1a. *Podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę.*

Zarządzeniem nr 30/2024 z dnia 31.12.2024 r. wprowadzona została *Instrukcja kancelaryjna w Centrum Informatycznym Edukacji* (dalej: instrukcja kancelaryjna) określająca szczegółowe zasady i tryb wykonywania czynności kancelaryjnych w CIE oraz regulująca postępowanie w tym zakresie z wszelką dokumentacją, począwszy od wpływu lub powstania dokumentacji wewnątrz CIE do momentu jej uznania za część dokumentacji w archiwum zakładowym lub przekazania do zniszczenia oraz niezależnie od techniki jej wytwarzania, postaci fizycznej oraz informacji w niej zawartych (§ 1 ust. 1 instrukcji kancelaryjnej). Zgodnie z § 2 ww. Instrukcji kancelaryjnej: Przy użytkowaniu systemów teleinformatycznych (innych niż EZD) przeznaczonych do realizacji określonych wyspecjalizowanych usług oraz spraw stosuje się przepisy niniejszej instrukcji. Dokumentacji gromadzonej i przetwarzanej w tych systemach nie ujmuje się w rejestrach przesyłek przychodzących, wychodzących i pism wewnętrznych, pod warunkiem, że w systemach tych możliwa jest analogiczna rejestracja, jaką przewidziano dla tych rejestrów w systemie EZD.

CIE udostępnia elektroniczną skrzynkę podawczą (dalej: ESP), spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji oraz zapewnia jej obsługę.

Od 1 stycznia 2025 r. wszedł w życie obowiązek stosowania e-Doręczeń przez podmioty publiczne[50], wskazane w ustawie z dnia 18 listopada 2020 r. *o doręczeniach elektronicznych*[51]. Podczas kontroli stwierdzono, że na stronie CIE pod adresem: https://cie.gov.pl/ został zamieszczony adres elektronicznej skrzynki podawczej CIE na ePUAP (/CIE/SkrytkaESP/) oraz adres doręczeń elektronicznych (AE:PL-40428-45235-SVERI-22).

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 5 ust. 2 pkt 1 ww. rozporządzenia KRI -*interoperacyjność na poziomie organizacyjnym osiągana jest przez informowanie przez podmioty realizujące zadania publiczne, w sposób umożliwiający skuteczne zapoznanie się, o sposobie dostępu oraz zakresie użytkowym serwisów dla usług realizowanych przez te podmioty*.

Na stronie internetowej CIE pod adresem https://cie.gov.pl/sio/ znajdują się informacje dotyczące danych oświatowych (informacje o szkołach i placówkach oświatowych, uczniach oraz kadrze pedagogicznej) oraz celu uzyskiwania danych oświatowych, tj. służących do: prowadzenia polityki edukacyjnej państwa na poziomie krajowym, regionalnym i lokalnym, funkcjonowania systemu finansowania zadań oświatowych (podziału części oświatowej subwencji ogólnej).
Na stronie zamieszczony został link do systemu dostępnego pod adresem: https://sio.gov.pl/sio/login.

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 15 ust. 2 ww. rozporządzenia KRI – *zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury*.

Deklarowany poziom świadczenia usług (ang. Service Level Agreement – SLA) Systemu Informacji Oświatowej został określony w OPZ, stanowiącym załącznik nr 2 do ww. umowy nr CIE-11/2024. SLA definiuje dostępność systemu, czas reakcji na awarię, procedury zgłaszania problemów i kary za niedotrzymanie warunków.
Zgodnie z zapisami zawartymi w OPZ (Rozdział 2. *Wprowadzenie)* poprzez utrzymanie w trybie produkcyjnym rozumie się dokonywanie wszelkich czynności technicznych w ramach świadczonej usługi, w szczególności:
- bieżące monitorowanie działania SIO i - w odpowiedzi na błędy - niezwłoczne podjęcie procedury zgodnie z SLA i warunkami gwarancji (pkt 1.3 lit. u) oraz
- zapewnienie wsparcia technicznego Service Desk dla realizowanej usługi zgodnie z wymaganymi przez Zamawiającego czasami SLA (Service Level Agreement) (pkt 1.3 lit. hh).

W ww. OPZ w Rozdziale 7. *Rozwiązywanie Awarii i Błędów*, pkt 7.2. *Obsługa zgłoszeń* zostały określone terminy usuwania zgłoszonych błędów (terminy realizacji SLA) w zależności od kategorii błędu.

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 16 ust. 1 ww. rozporządzenia KRI – *systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub*

[50] Zgodnie z Komunikatem Ministra Cyfryzacji z dnia 12 lipca 2024 r. *zmieniającym komunikat w sprawie określenia terminu wdrożenia rozwiązań technicznych niezbędnych do doręczania korespondencji z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej oraz udostępnienia w systemie teleinformatycznym punktu dostępu do usług rejestrowanego doręczenia elektronicznego w ruchu transgranicznym.*
[51] Dz.U. z 2026 r. poz. 3.

oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.

System Informacji Oświatowej wykorzystywany do realizacji zadań publicznych umożliwia wymianę danych z innymi systemami teleinformatycznymi m.in.: Krajowym Systemem Danych Oświatowych (KSDO), Zintegrowaną Platformą Edukacyjną (ZPE), rejestrem PESEL, REGON, Profilem Zaufanym/Krajowym Węzłem Identyfikacji Elektronicznej, mLegitymacją.

Zgodnie z art. 97 ust. 2 ustawy *o systemie informacji oświatowej* do zabezpieczenia poufności przekazywania danych do bazy danych SIO i pozyskiwania danych z bazy danych SIO wykorzystuje się mechanizmy szyfrowania danych.

Opracowana przez CIE *Polityka Wytwarzania Oprogramowania*[52] zawiera zapisy dotyczące wymagań bezpieczeństwa systemów, wskazując m.in., że „systemy muszą być projektowane i utrzymywane w sposób zapewniający interoperacyjność z innymi systemami, zgodnie z obowiązującymi Krajowymi Ramami Interoperacyjności. Wymaga się stosowania standardowych formatów danych, protokołów komunikacji oraz mechanizmów zapewniających integralność i autoryzację przesyłanych informacji" (cz. 10, pkt 9). „Stosowane algorytmy kryptograficzne muszą być zgodne z aktualnymi wytycznymi NIST[53], w szczególności z zatwierdzonymi rodzinami SHA-2 (np. SHA-256, SHA-512) lub SHA-3, zapewniając wysokie bezpieczeństwo danych" (cz. 10, pkt 14).

Zgodnie z informacją[54] przekazaną przez Zastępcę Dyrektora CIE „system został wyposażony w składniki sprzętowe oraz oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi z wykorzystaniem protokołów komunikacyjnych i mechanizmów szyfrujących zgodnych z obowiązującymi przepisami, normami i standardami. W szczególności stosowane są:

a) protokół HTTPS z wykorzystaniem TLS – w zakresie komunikacji użytkowników z portalem,
b) algorytmy kryptograficzne (...) – w ramach połączeń administracyjnych z serwerami systemu,
c) certyfikaty SSL/TLS – wykorzystywane w integracjach z innymi systemami teleinformatycznymi".

W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 17 ust. 1 ww. rozporządzenia KRI – *kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą.*

[52] Symbol dokumentu: CIE/SZBI/PWO, data wydania dokumentu: 9.01.2026 r., wersja 2.0.
[53] NIST (ang.) National Institute of Science and Technology;
Departament Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów opracował dokument pn. Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego Część II, opracowany na podstawie publikacji amerykańskiego NIST, dostępny pod adresem: https://www.gov.pl/attachment/1aaca106-fb4f-4831-989a-1e75da59d42d
[54] Pismo CIE z 3 lutego 2026 r., znak: ZPiA.061.1.2025.

Zgodnie z wyjaśnieniami[55] Zastępcy Dyrektora CIE „kodowanie znaków w dokumentach wysyłanych oraz odbieranych przez system odbywa się zgodnie ze standardem Unicode UTF-8".
Na podstawie instrukcji technicznej SIO[56] oraz Bazy wiedzy SIO – Confluence[57] ustalono, że System Informacji Oświatowej wymaga stosowania standardu kodowania znaków Unicode UTF-8 dla poprawnego przetwarzania danych, w szczególności podczas importu plików (np. CSV/XVSIO) oraz wymiany danych z systemami dziedzinowymi.
W badanym zakresie nie stwierdzono nieprawidłowości.

- Zgodnie z § 18 ww. rozporządzenia KRI:

ust. 1. *Systemy teleinformatyczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia KRI.*

ust. 2. *Jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia.*

Zastępca Dyrektora CIE przedstawił następującą informacje[58]: „system udostępnia zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności. W ramach systemu wykorzystywane są następujące formaty danych/rozszerzenia plików: .html, .css, .js, .jpg, .png, .svg, .xml, .xsd. (…) system umożliwia przyjmowanie dokumentów elektronicznych służących do realizacji zadań należących do jego zakresu działania w formatach danych określonych w załącznikach nr 2 i 3 do ww. rozporządzenia KRI. W szczególności system obsługuje import danych w formatach .csv oraz .xml. (…)".

Dodatkowo Zastępca Kierownika Zakładu Projektowania i Analiz w wyjaśnieniach[59] wskazała: „Należy zaznaczyć, że formaty .html, .css oraz .js zostały wskazane jako formaty wykorzystywane przez system na potrzeby jego działania i prezentacji treści w środowisku przeglądarkowym. Nie są one jednak udostępniane użytkownikom jako formaty wymiany danych ani nie służą do realizacji procesów importu lub eksportu danych. Z punktu widzenia użytkownika końcowego wymiana danych realizowana jest w formatach dedykowanych do tego celu, w szczególności .xml zgodnym z odpowiednimi schematami .xsd".
Do powyższych wyjaśnień zostały dołączone dokumenty potwierdzające wykorzystywane przez SIO ww. formaty danych, tj.:

- rejestracja danych identyfikacyjnych uczniów i nauczycieli; eksport listy umów nauczycieli, dla których rejestrowane jest wynagrodzenie – format .csv;
- rejestracja listy legitymacji szkolnych i przedszkolnych (funkcjonalność mLegitymacji) – format .jpg;
- import legitymacji – format .xml;
- wykaz formatów danych/rozszerzeń nazw plików zapewniających dostęp do zasobów informacji udostępnianych za pomocą SIO – formaty html, css, js, json, png, svg, csv, jpg, xml, xsd.

---

[55] Pismo CIE z 3 lutego 2026 r., znak: ZPiA.061.1.2025.
[56] dostępnej pod adresem: https://pomoc.sio.gov.pl/tech_instruction/tworzenie-pliku-csv-oraz-import-danych-3/
[57] dostępnej pod adresem: https://pomoc-ksdo.atlassian.net/wiki/spaces/BWSIO/pages/12360580/Tworzenie+pliku+CSV+oraz+import+danych+-+JST+-+uczniowie
[58] Jw.
[59] Wiadomość elektroniczna (e-mail) z 3.06.2026 r. wraz z załącznikami.

W badanym zakresie nie stwierdzono nieprawidłowości.

Podczas kontroli wystąpiono[60] o przekazanie dokumentów potwierdzających spełnianie wymagań określonych w § 16 ust. 1, § 17 ust. 1, § 18, § 19 ust. 4 rozporządzenia KRI. W odpowiedzi Zastępca Dyrektora CIE przekazał następującą informację:
„Jednocześnie informuję, że dokumentacja techniczna i projektowa systemu prowadzona jest w sposób ciągły i funkcjonalny. Część informacji znajduje się w repozytorium kodu źródłowego (w szczególności w zakresie konfiguracji technicznej, mechanizmów bezpieczeństwa oraz integracji), natomiast pozostałe elementy stanowią część analizy biznesowo-systemowej, prowadzonej na potrzeby realizacji i rozwoju systemu. W związku z powyższym nie wszystkie informacje występują w postaci odrębnych, sformalizowanych dokumentów. (…)".

Ocena cząstkowa badanego obszaru: pozytywna.

***Audyt kodu źródłowego Systemu Informacji Oświatowej (SIO)* - ekspertyza wykonana na podstawie umowy zawartej w dniu 6 czerwca 2025 r. pomiędzy Centrum Informatycznym Edukacji a Polskim Towarzystwem Informatycznym**

W okresie objętym kontrolą, tj. od 1 stycznia 2025 r. do 30 września 2025 r. w CIE został przeprowadzony zewnętrzny audyt kodu źródłowego SIO[61]. W wyniku przeprowadzonego audytu został sporządzony 20 listopada 2025 r. dokument pn. *Raport audytu kodu źródłowego Systemu Informacji Oświatowej (SIO)*, zawierający rekomendacje działań związanych z utrzymaniem i rozwojem SIO.
W ramach ww. audytu zostały wykonane następujące zadania[62]:

1) analiza szczegółowej dokumentacji kodu źródłowego – dokonano analizy, które obszary dokumentacji wymagają uzupełnienia lub aktualizacji, a także oceniono czy dokumentacja jest zgodna z rzeczywistym stanem aplikacji, procesami wytwarzania oprogramowania, konfiguracją środowiska i integracjami z systemami zewnętrznymi;
2) weryfikacja kodu, bibliotek, „frameworków" (środowisk projektowych) oraz praktyk programistycznych, pod kątem aktualnych wersji systemów operacyjnych, przeglądarek internetowych i możliwości integracji kodu z innymi zewnętrznymi usługami wskazanymi przez CIE – dokonano oceny czy oprogramowanie korzysta z aktualnych, wspieranych technologii oraz sprawdzenie, czy nie występują złe praktyki programistyczne, jak np. „hardcoding" wartości, nadmierna złożoność funkcji czy duplikacja logiki;
3) sprawdzenie czy kod jest spójny, czytelny i zrozumiały dla potencjalnych nowych Wykonawców;
4) weryfikacja czy funkcje systemu spełniają przyjęte praktyki oraz wymagania zawarte w dokumentacji CIE;
5) propozycja zmian w sposobie wytwarzania oprogramowania w celu zachowania jego poprawnej struktury, uniknięcia technicznych długów i zwiększenia łatwości utrzymania aplikacji, bez zmiany jej zachowań;
6) weryfikacja czy konfiguracja jest łatwa do zmiany i nie wprowadza ryzyka błędów w produkcji;

[60] Pismo MEN z 27.01.2026 r., znak: DWST-WDiR.0915.1.2025.AJK2.
[61] Umowa zawarta w dniu 6 czerwca 2025 r. pomiędzy Centrum Informatycznym Edukacji a Polskim Towarzystwem Informatycznym.
[62] Audytowane zadania zostały opisane w *Raporcie audytu kodu źródłowego Systemu Informacji Oświatowej (SIO)* w części 2. Cel ekspertyzy, pkt 2.1.Przedmiot badania (audytu).

7) ocena oprogramowania pod względem stabilności i skalowalności aplikacji do dalszego rozwoju.

Wyniki przeprowadzonego audytu kodu źródłowego Systemu Informacji Oświatowej zawierają m.in. ocenę oprogramowania pod względem stabilności i skalowalności systemu do dalszego rozwoju[63].
W Rozdziale 13. Podsumowanie i wnioski końcowe ww. *Raportu* zawarto, że „przeprowadzona analiza wykazała, że System Informacji Oświatowej (SIO) boryka się z problemami cechującymi systemy, których budowa rozpoczęła się wiele lat temu, a przez lata skupiono się jedynie na ich utrzymaniu i nadążnym aktualizowaniu w zakresie wymagań funkcjonalnych (…)". Wskazano czynniki mające wpływ na wzrost niepewności w zakresie dalszego utrzymania i rozwoju systemu.
Zespół rzeczoznawców Polskiego Towarzystwa Informatycznego przedstawił w ww. *Raporcie* rekomendacje dotyczące podjęcia działań związanych z utrzymaniem i rozwojem systemu SIO, w tym rekomendował opracowanie szczegółowego planu naprawczego.

Od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

Z upoważnienia
Ministra Edukacji

Marek Kuciński
Dyrektor
/ – podpisano cyfrowo/

[63] Na podstawie raportu z audytu kodu źródłowego Systemu Informacji Oświatowej (SIO) z 20 listopada 2025 r. (Rozdział 11. Uwagi i spostrzeżenia, pkt 11.7. Perspektywa rozwoju).

Potwierdzam zgodność kopii wydruku z dokumentem elektronicznym:

Identyfikator dokumentu	3160636.13079205.11139201
Nazwa dokumentu	2026.07.14 Wystąpienie pokontrolne - Centrum Informatyczne Edukacji.docx
Tytuł dokumentu	2026.07.14 Wystąpienie pokontrolne - Centrum Informatyczne Edukacji
Sygnatura dokumentu	DWST-WDiR.0915.1.2025.AJK
Data dokumentu	14.07.2026
Skrót dokumentu	0B04B26CCC5FA5AF47187896B2A708A5FB495ADF
Wersja dokumentu	1.2
Data podpisu	14.07.2026 13:15:36
Podpisane przez	Marek Kuciński Dyrektor
Rodzaj certyfikatu	Certyfikat kwalifikowany podpisu elektronicznego

EZD 3.134.5.5.

Data wydruku: 14.07.2026

Autor wydruku: Jakubiak-Kępińska Alicja (Radca)