VI Kadencja

Tryb obiegowy

Uchwała nr 322/VI/2026
Krajowej Rady Diagnostów Laboratoryjnych
z dnia 23 września 2026 roku
w sprawie przyjęcia przez Krajową Izbę Diagnostów Laboratoryjnych
Systemu Zarządzania Bezpieczeństwem Informacji

Na podstawie art. 81 ust. 1 i 5, art. 88 pkt 13 i 14 ustawy z dnia 15 września 2022 r. o medycynie laboratoryjnej (Dz. U. z 2025 r. poz. 1295), w związku z § 20 ust. 2 pkt 25 i 27 Statutu Krajowej Izby Diagnostów Laboratoryjnych, stanowiącego załącznik do Uchwały nr 28/2022 VI Krajowego Zjazdu Diagnostów Laboratoryjnych z dnia 16 grudnia 2022 roku w sprawie Statutu Krajowej Izby Diagnostów Laboratoryjnych, oraz w związku z Zarządzeniem nr 13/2025 Prezesa Krajowej Rady Diagnostów Laboratoryjnych z dnia 01 grudnia 2025 roku w sprawie pilotażowego przygotowania do wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Krajowej Izbie Diagnostów Laboratoryjnych, Krajowa Rada Diagnostów Laboratoryjnych uchwala, co następuje:

§ 1

1. Przyjmuje się do stosowania w Krajowej Izbie Diagnostów Laboratoryjnych System Zarządzania Bezpieczeństwem Informacji, stanowiący strategię działania w zakresie zabezpieczenia właściwej ochrony informacji oraz w celu zapewnienia efektywnego zarządzania bezpieczeństwem, ochroną poufności, dostępności i integralności danych Izby.
2. System Zarządzania Bezpieczeństwem Informacji definiuje zasady, procedury i mechanizmy mające na celu:
    1) ochronę poufności, integralności, rozliczalności i dostępności informacji;
    2) zgodność z obowiązującymi przepisami prawa oraz standardami obowiązującymi w Krajowej Izbie Diagnostów Laboratoryjnych, mając na uwadze charakter prowadzonej działalności, jako samorządu zawodowego;
    3) minimalizację ryzyka związanego z zagrożeniami informacyjnymi;
    4) zapewnienie ciągłości działania organizacji w przypadku wystąpienia incydentów;
    5) wdrożenie i utrzymanie adekwatnych do zagrożeń i wyników szacowania ryzyka zabezpieczeń organizacyjnych i technicznych;
    6) umożliwienie efektywnego przeprowadzania przeglądów aktualizacyjnych polityk i procedur.

§ 2

1. Krajowa Rada Diagnostów Laboratoryjnych udziela upoważnienia Prezes Krajowej Rady Diagnostów Laboratoryjnych do określenia w drodze odrębnych Zarządzeń:

1) szczegółowej treści Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, mając na względzie cele określone w § 1 ust. 2 Uchwały, obowiązków, standardów i wymagań wynikających w szczególności z Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 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), Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, oraz Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne w takim zakresie, w jakim znajdują one zastosowanie do Krajowej Izby Diagnostów Laboratoryjnych;
2) szczegółowych procedur Zarządzania Bezpieczeństwem Informacji, Technicznych i Operacyjnych, Fizycznych i Środowiskowych, procedur Zarządzania Dostawcami, Ciągłości Działania, Edukacji i Szkoleń oraz Procedur Zgodności i Audytów.

2. Prezes Krajowej Rady Diagnostów Laboratoryjnych określa szczegółową treść Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji oraz stosowne procedury, o których mowa wyżej w drodze Zarządzeń w terminie 14 dni od dnia wejścia w życie Uchwały.

§ 3

Uchwała wchodzi w życie z dniem podjęcia.

Niniejsza uchwała została podjęta przy udziale 23 członków Krajowej Rady Diagnostów Laboratoryjnych na ogólną liczbę 38 członków:

1) za uchwałą – 23
2) przeciw uchwale – 0
3) wstrzymało się – 0

Imienny wykaz głosów stanowi załącznik do uchwały.

Prezes KRDL

dr n. med. Monika Pintal-Ślimak

UZASADNIENIE

System Zarządzania Bezpieczeństwem Informacji (SZBI) w Krajowej Izbie Diagnostów Laboratoryjnych. stanowi podsumowanie prac analitycznych i organizacyjnych w obszarze IT oraz bezpieczeństwa, prowadzonych systematycznie od 2023 roku. Fundamentem dla budowy spójnego systemu były kompleksowo obsłużone w 2023 i na początku 2024 roku kluczowe obszary organizacyjne i formalno-prawne. W ramach tych prac wdrożono szereg wewnętrznych regulacji, stanowiących przygotowanie i podwaliny pod realizację i wprowadzenie kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji, to jest między innymi: zarządzenie nr 2/2023 z dnia 20 kwietnia 2023 r. w sprawie rejestru umów KIDL, uchylone przez zarządzenie nr 11/2024 z dnia 28 sierpnia 2024 r. w sprawie rejestru umów Krajowej Izby Diagnostów Laboratoryjnych, zarządzenie nr 15/2023 z dnia 25 października 2023 r. w sprawie przyjęcia Instrukcji Ochrony w Krajowej Izbie Diagnostów Laboratoryjnych, a także zarządzenie nr 22/2023 z dnia 30 listopada 2023 r. w sprawie wprowadzenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych KIDL. Równolegle wdrożono zarządzenie nr 18/2023 z dnia 6 listopada 2023 r. w sprawie przeprowadzenia okresowej inwentaryzacji składników majątkowych za rok 2023, która stanowiła niezbędną bazę do przeprowadzenia inwentaryzacji aktywów teleinformatycznych na potrzeby analizy ryzyka. Uzupełnieniem powyższych działań było wydanie zarządzenia nr 23/2023 z dnia 30 listopada 2023 r. w sprawie wprowadzenia do stosowania polityki zarządzania kluczami do archiwum w siedzibie KIDL. Powyższe działania organizacyjne, połączone z weryfikacją stanu realizacji zaleceń z audytu IT, umożliwiły w czwartym kwartale 2024 roku formalne przejście do prac nad kompleksowym SZBI.

W pierwszym kwartale 2025 roku opracowano harmonogram działań operacyjnych oraz przygotowano pierwszą wersję roboczą SZBI. Wykonano również szczegółową analizę wymagań dla obszaru IT, która stanowiła merytoryczną podstawę do przygotowania wniosków o dofinansowanie. W drugim kwartale 2025 roku przeprowadzono audyt obowiązujących umów z dostawcami usług IT pod kątem ich zgodności z wymaganiami projektowanego systemu. Wyniki analizy stanowiły podstawę do optymalizacji kosztów utrzymania infrastruktury i wypowiedzenia ówczesnych kontraktów. Działanie to umożliwiło organizację nowego procesu wyboru dostawców. W trzecim kwartale 2025 roku zawarto umowy na nowych warunkach. Załączniki do dokumentów zobowiązały dostawców usług chmurowych, hostingu oraz obsługi IT do stosowania procedur zgodnych z opracowywanym SZBI. Wprowadzono wymóg realizacji parametrów SLA, stosowania uwierzytelniania wieloskładnikowego (MFA) oraz określono czasy zgłaszania incydentów w przedziale od 4 do 24 godzin od ich wykrycia. W tym samym okresie zainicjowano integrację systemów wewnętrznych z rozwiązaniami Ministerstwa Cyfryzacji oraz Ministerstwa Zdrowia.

Na przełomie lat 2025 i 2026 do dokumentacji SZBI włączono mechanizmy mitygacji zidentyfikowanych ryzyk technologicznych i prawnych. W związku z rozwojem modeli algorytmicznych zdefiniowano zjawisko nieautoryzowanego użycia sztucznej inteligencji. Ustanowiono zasady korzystania z zatwierdzonych systemów sztucznej inteligencji oraz określono zakaz wprowadzania danych wewnętrznych

do systemów publicznych. W kwietniu 2026 roku weszła w życie nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa, implementująca dyrektywę NIS2. Organizacja, jako podmiot objęty tymi regulacjami, wdrożyła proces raportowania incydentów bezpieczeństwa do CSIRT NASK w wyznaczonych ustawowo interwałach czasowych.

Uchwała umożliwia zapewnienie, aby architektura SZBI funkcjonująca w Krajowej Izbie Diagnostów Laboratoryjnych funkcjonowała w modelu ciągłego doskonalenia i zachowywała zgodność z wytycznymi norm ISO/IEC 27000 oraz NIST, uwzględniała wymogi Ogólnego Rozporządzenia o Ochronie Danych (RODO), rozporządzenia Data Act oraz Krajowych Ram Interoperacyjności. Równocześnie, ze względu na szeroki aspekt techniczny, wymagane i pożądane jest, aby praca na procedurach i dokumentach związanych z Systemem Zarządzania Bezpieczeństwem Informacji uwzględniała konieczność dynamicznego ich dostosowywania do praktycznego charakteru ich stosowania. Upoważnienie Prezes Krajowej Rady Diagnostów Laboratoryjnych do określania zasad i procedur dotyczących Bezpieczeństwa Informacji w drodze odrębnych Zarządzeń pozwala osiągnąć wyżej wymieniony cel.

System opiera się na dokumencie głównym i siedmiu grupach procedur wykonawczych, regulujących zarządzanie ryzykiem, incydentami, ciągłością działania oraz bezpieczeństwem fizycznym i środowiskowym. Infrastruktura IT, procesy organizacyjne oraz relacje z dostawcami zostały dostosowane do zatwierdzenia i formalnego wdrożenia systemu w jego ostatecznym kształcie.

Id	Nazwa	Głosuję nad podjęciem uchwały w sprawie przyjęcia przez Krajową Izbę Diagnostów Laboratoryjnych Systemu Zarządzania Bezpieczeństwem Informacji;
1	Ewa Brzezińska	za
2	Katarzyna Fischer	za
3	Wojciech Markiewicz	za
4	Liliana Guzik	za
5	Joanna Kowalska	za
6	Mateusz Chmielarz	za
7	Alicja Utracka	za
8	Sylwia Kozłowska	za
9	Aldona Wierzbicka-Ruciń	za
10	Elżbieta Rabsztyn	za
11	Monika Jabłonowska	za
12	Konrad Grzeszczak	za
13	Monika Pintal-Ślimak	za
14	Sylwester Łużny	za
15	Magdalena Frankiewicz	za
16	Renata Krygier	za
17	Piotr Brzyśkiewicz	za
18	Anna Lipnicka	za
19	Katarzyna Ziółkowska	za
20	Karolina Bukowska-Strak	za
21	Sylwia Moskwa	za
22	Jacek Pulit	za
23	Małgorzata Wojtkowska	za