

„ZATWIERDZAM”

DYREKTOR
DEPARTAMENTU CYBERBEZPIECZEŃSTWA

.....
(podpis, data)
Paweł DZIUBA

REGULAMIN

Projektu Akademia_CYBER.MIL w roku akademickim 2025/2026

§ 1. Postanowienia ogólne dotyczące realizacji Projektu

1. Podstawą wdrożenia Projektu Akademia_CYBER.MIL (dalej: Projekt) jest niepublikowana *Decyzja Nr 304/DC Ministra Obrony Narodowej z dnia 8 września 2025 r. w sprawie realizacji Projektu Akademia_CYBER.MIL w roku akademickim 2025/2026*, dotycząca wsparcia cywilnych uczelni w procesie kształcenia na kierunkach związanych z obszarem informatyki i cyberbezpieczeństwa.
2. Organizatorem Projektu jest Minister Obrony Narodowej, reprezentowane przez Departament Cyberbezpieczeństwa i Eksperckie Centrum Szkolenia Cyberbezpieczeństwa (dalej: DC, ECSC tj. Organizatorzy).
3. Celem głównym Projektu jest popularyzowanie wizerunku Sił Zbrojnych Rzeczypospolitej Polskiej oraz jednostek organizacyjnych resortu obrony narodowej (dalej: ron), jako atrakcyjnego i innowacyjnego miejsca do podjęcia pracy i służby oraz rozwoju kariery zawodowej dla ekspertów z obszaru informatyki i cyberbezpieczeństwa.
4. Projekt w roku akademickim 2025/2026 skierowany jest do wszystkich chętnych politechnik oraz wyższych uczelni technicznych na obszarze całej Rzeczypospolitej Polskiej, będących uczelniami publicznymi, które kształcą na kierunkach technicznych, związanych z szeroko rozumianym obszarem informatyki i cyberbezpieczeństwa, które w terminie do dnia 17 października 2025 r. poprzez stronę ECSC <https://ecsc.mil.pl/> (w zakładce dedykowanej Projektowi) wypełnią deklarację chęci udziału w przedmiotowym Projekcie.
5. W ramach Projektu przewiduje się:
 - 1) wsparcie merytoryczne udzielone przez ECSC oraz inne komórki i jednostki organizacyjne ron, zaangażowane w proces kształcenia oraz szkolenia w obszarze informatyki i cyberbezpieczeństwa;
 - 2) inspirowanie środowiska akademickiego uczestniczącego w Projekcie do angażowania się w realizację Projektu „Zostań Żołnierzem Rzeczypospolitej” oraz ochotniczego szkolenia wojskowego studentów i absolwentów uczelni wyższych w ramach programu Legii Akademickiej.
6. W ramach Projektu zakłada się trzy etapy:
 - a) e-learningowe kursy w obszarze informatyki i cyberbezpieczeństwa,
 - b) ogólnopolskie zdalne zawody Capture The Flag (dalej: CTF),
 - c) ogólnopolskie stacjonarne zawody CTF.

7. Zakłada się udostępnienie dla studentów uczelni biorących udział w Projekcie (osób kształcących się na studiach pierwszego lub drugiego stopnia albo jednolitych studiach magisterskich) oraz posiadających obywatelstwo polskie w okresie od listopada 2025 r. do lutego 2026 r. na wydzielonej i zarządzanej przez ECSC platformie e-learningowej, certyfikowanych kursów z obszaru informatyki i cyberbezpieczeństwa.
8. Kursy udostępnione będą wg poniższego harmonogramu:
 - 1) Kurs Junior Cybersecurity Analyst (platforma CISCO Networking Academy) — w okresie od dnia 3 listopada 2025 r. do dnia 22 listopada 2025 r.
 - 2) Kurs CyberOps Associate (platforma CISCO Networking Academy) — w okresie od dnia 1 grudnia 2025 r. do dnia 20 grudnia 2025 r.
 - 3) Kurs Zarządzanie zasobami Data Center z wykorzystaniem CISCO Intersight (platforma ECSC) — w okresie od dnia 5 stycznia 2026 r. do dnia 23 stycznia 2026 r.
 - 4) Techniki zapewnienia ciągłości pracy i przywracania po awarii w centrach danych (platforma ECSC) — w okresie od dnia 2 lutego 2026 r. do dnia 20 lutego 2026 r.
9. Każdy z kursów zakończony będzie testem wiedzy. Do zaliczenia testu konieczne jest udzielenie 70% poprawnych odpowiedzi.
10. Po uzyskaniu pozytywnego wyniku z testu wiedzy po każdym z kursów będzie możliwość wygenerowania zaświadczenia o jego ukończeniu po wcześniejszym wypełnieniu ankiety satysfakcji.
11. Zainteresowani studenci będą mieli możliwość wzięcia udziału w dowolnej liczbie kursów.
12. Studenci zainteresowani wzięciem udziału w Projekcie zgłaszają się do wyznaczonego przez Rektora koordynatora uczelnianego. Informację w tej sprawie posiada Biuro Karier na uczelni.
13. W celu dostępu do platformy studenci biorący udział w Projekcie będą używać adresów e-mail z domeną uczelni.
14. Przed terminem udostępnienia danego kursu na platformie e-learningowej, na wskazane przez studentów zgłoszonych do udziału w Projekcie adresy e-mail z domeną uczelni, zostaną przesłane linki z instrukcją dostępu do danego kursu, który można realizować w częściach, przez cały okres jego trwania, zgodnie z harmonogramem, o którym mowa w pkt 8.
15. Rozpoczęcie procesu każdego szkolenia określonego w Projekcie rozpoczyna się poprzez zalogowanie i zapoznanie z zamieszczonymi materiałami na platformie e-learningowej MOODLE-ECSC.
16. Aby zalogować się do Platformy CISCO NETACAD należy użyć linka umieszczonego na platformie e-learningowej MOODLE-ECSC. W następnym kroku rozpocznie się proces samodzielnego założenia konta i przypisania dostępu do szkolenia. Po wykonaniu opisanej procedury uczestnicy szkolenia pracują oraz zdają egzamin w sposób indywidualny w ramach określonego harmonogramu.
17. Warunkiem koniecznym do zakończenia szkolenia jest wypełnienie ankiety zamieszczonej na platformie MOODLE-ECSC, po jego zakończeniu.

§ 2. Zasady organizacji ogólnopolskich zdalnych zawodów CTF

1. Organizatorem ogólnopolskich zdalnych zawodów CTF jest Ministerstwo Obrony Narodowej, reprezentowane przez Departament Cyberbezpieczeństwa i Eksperckie Centrum Szkolenia Cyberbezpieczeństwa (dalej: Organizatorzy).
2. W okresie od dnia 9 marca 2026 r. do dnia 10 kwietnia 2026 r. zorganizowane zostaną przez DC i ECSC ogólnopolskie zdalne zawody CTF.
3. Ogólnopolskie zdalne zawody CTF będą polegały na wykonaniu jak największej ilości zadań z zakresu cyberbezpieczeństwa w wyznaczonym czasie.
4. W ogólnopolskich zdalnych zawodach CTF udział wezmą pięcioosobowe zespoły reprezentujące wszystkie chętne uczelnie biorące udział w Projekcie.

5. W skład zespołów będą wchodzić studenci danej uczelni (osoby kształcące się na studiach pierwszego lub drugiego stopnia albo jednolitych studiach magisterskich) posiadający obywatelstwo polskie oraz wykazujący się szczególnymi osiągnięciami w obszarze informatyki i cyberbezpieczeństwa.
6. Ustalenie składu zespołów biorących udział w ogólnopolskich zdalnych zawodach CTF pozostawia się w gestii władz poszczególnych uczelni.
7. W terminie do dnia 2 marca 2026 r. uczelnie na wydzielonej i zarządzanej przez ECSC platformie e-learningowej wskażą skład zespołów CTF (nazwa uczelni, imiona i nazwiska studentów, e-maile studentów z domeną uczelni, numery kontaktowe telefonów studentów oraz wskazanie lidera zespołu).
8. Kwalifikacji uczelni do ogólnopolskich zdalnych zawodów CTF dokona ECSC we współpracy z DC.
9. DC poinformuje Uczelnie, które zakwalifikowały się do ogólnopolskich zdalnych zawodów CTF.
10. Równoległe lista Uczelni zakwalifikowanych do ogólnopolskich zdalnych zawodów CTF zostanie opublikowana na stronie ECSC.
11. W ramach prowadzonych ogólnopolskich zdalnych zawodów CTF zespoły będą rywalizowały między sobą, gromadząc punkty w różnych konkurencjach na konto swojej drużyny.
12. Studenci wytypowani do zespołów reprezentujących uczelnie, przed przystąpieniem do ogólnopolskich zdalnych zawodów CTF będą musieli podpisać oświadczenie o zapoznaniu się z regulaminem Projektu Akademia_CYBER.MIL (załącznik nr 1).
13. Uczestnicy ogólnopolskich zdalnych zawodów CTF korzystają z własnych komputerów (zawody online z terytorium Polski). Konieczne jest posiadanie w komputerze przenośnym (notebooku) karty sieciowej, Ethernet, 100/1000Mbit/s ze złączem RJ45 i ewentualnie w przypadku chęci skorzystania z dodatkowego monitora posiadania złącza HDMI. Preferowany system operacyjny komputerów to Kali Linux lub ewentualnie maszyna wirtualna z tym systemem.
14. Warunkiem uczestnictwa w ogólnopolskich stacjonarnych zawodach CTF jest:
 - 1) ukończenie przez studenta w dniu rozpoczęcia zawodów 18 lat;
 - 2) posiadanie obywatelstwa polskiego;
 - 3) posiadanie pełnej zdolności do czynności prawnych
(wzór Oświadczenia określony w Załączniku nr 1 do Regulaminu).
15. Przed przystąpieniem do udziału w ogólnopolskich stacjonarnych zawodach CTF uczestnik powinien zapoznać się z niniejszym Regulaminem dostępnym u koordynatorów uczelnianych Projektu oraz na stronie internetowej www.ecsc.mil.pl.
16. Udział w ogólnopolskich stacjonarnych zawodach CTF jest równoznaczny z akceptacją Regulaminu.
17. Wyniki z ogólnopolskich zdalnych zawodów CTF zostaną opublikowane na stronie internetowej ECSC.
18. Maksymalnie szesnaście zespołów uczelnianych, które otrzymają najwyższą punktację podczas ogólnopolskich zdalnych zawodów CTF, zakwalifikuje się do ogólnopolskich stacjonarnych zawodów CTF.

§ 3. Zasady organizacji ogólnopolskich stacjonarnych zawodów CTF

1. Organizatorem ogólnopolskich stacjonarnych zawodów CTF jest Ministerstwo Obrony Narodowej, reprezentowane przez Departament Cyberbezpieczeństwa i Eksperckie Centrum Szkolenia Cyberbezpieczeństwa (dalej: Organizatorzy).
2. Ogólnopolskich stacjonarnych zawodów CTF odbędzie się w dniu 6 maja 2026 r. w Centrum Konferencyjnym Wojska Polskiego (ul. Żwirki i Wigury 9/13, 02-143 Warszawa). Oficjalne rozpoczęcie ogólnopolskich stacjonarnych zawodów CTF nastąpi o godz.: 8:00.

3. W dniu zawodów należy stawić się w miejscu wskazanym w pkt 2 o godz.: 7:00, z dokumentem potwierdzającym tożsamość, w celu rejestracji i pobrania pakietu startowego (materiały promocyjne).
4. Organizatorzy zastrzegają sobie prawo do zmiany terminu ogólnopolskich stacjonarnych zawodów CTF, jeśli taka zmiana będzie uzasadniona względami organizacyjnymi.
5. Przyjazd na ogólnopolskie stacjonarne zawody CTF i ewentualny nocleg uczestnicy organizują we własnym zakresie.
6. Ogólnopolskie stacjonarne zawody CTF skierowane są do studentów uczelni zakwalifikowanych do udziału w Projekcie.
7. Każda uczelnia wystawia jeden zespół.
8. Maksymalnie szesnaście zespołów uczelnianych, które otrzymają najwyższą punktację podczas ogólnopolskich zdalnych zawodów CTF, zakwalifikuje się do ogólnopolskich stacjonarnych zawodów CTF.
9. Ustalenie składu zespołów biorących udział w ogólnopolskich stacjonarnych zawodów CTF pozostawia się w gestii władz poszczególnych uczelni.
10. W ogólnopolskich stacjonarnych zawodach CTF udział wezmą pięcioosobowe zespoły reprezentujące uczelnie biorące udział w Projekcie.
11. W skład zespołów biorących udział w ogólnopolskich stacjonarnych zawodach CTF będą wchodzić studenci danej uczelni (osoby kształcące się na studiach pierwszego lub drugiego stopnia albo jednolitych studiach magisterskich) posiadający obywatelstwo polskie oraz wykazujący się szczególnymi osiągnięciami w obszarze informatyki i cyberbezpieczeństwa.
12. Każdy zespół może wycofać się z ogólnopolskich stacjonarnych zawodów CTF, w dowolnym czasie. Wycofanie jest równoznaczne z utratą prawa do nagród, o których mowa w pkt 50-51.
13. W terminie do dnia 20 kwietnia 2026 r. uczelnie na wydzielonej i zarządzanej przez ECSC platformie e-learningowej wskażą skład zespołów ogólnopolskich stacjonarnych zawodów CTF, (nazwa uczelni, imiona i nazwiska studentów, e-maile studentów z domeną uczelni, numery kontaktowe studentów oraz wskazanie lidera zespołu).
14. Weryfikacji zespołów dokona ECSC we współpracy z DC.
15. DC poinformuje Uczelnie o zakwalifikowaniu do ogólnopolskich stacjonarnych zawodów CTF.
16. Równolegle, lista Uczelni zakwalifikowanych do ogólnopolskich stacjonarnych zawodów CTF zostanie opublikowana na stronie ECSC.
17. Ogólnopolskie stacjonarne zawody CTF będą polegały na wykonaniu jak największej ilości zadań z zakresu cyberbezpieczeństwa w wyznaczonym czasie.
18. W ramach prowadzonych ogólnopolskich stacjonarnych zawodów CTF zespoły będą rywalizowały między sobą, gromadząc punkty w różnych konkurencjach na konto swojej drużyny.
19. Studenci wytypowani do zespołów reprezentujących uczelnie, przed przystąpieniem do ogólnopolskich stacjonarnych zawodów CTF, będą musieli podpisać oświadczenie o zapoznaniu się z regulaminem.
20. Poza zadaniami wskazanymi przez organizatorów do wykonania przy stanowiskach komputerowych w ramach ogólnopolskich stacjonarnych zawodów CTF, zespoły będą miały możliwość zdobycia dodatkowych punktów w rywalizacjach na strzelnicy wirtualnej, którą zabezpieczy Centralne Wojskowe Centrum Rekrutacji (dalej: CWCR). Punkty te będą brane pod uwagę w przypadku tej samej liczby punktów zdobytych podczas ogólnopolskich stacjonarnych zawodów CTF.
21. Warunkiem uczestnictwa w ogólnopolskich stacjonarnych zawodach CTF jest:
 - 1) ukończenie przez studenta w dniu rozpoczęcia zawodów 18 lat;

- 2) posiadanie obywatelstwa polskiego;
 - 3) posiadanie pełnej zdolności do czynności prawnych
(wzór Oświadczenia określony w Załączniku nr 1 do Regulaminu).
22. Przed przystąpieniem do udziału w ogólnopolskich stacjonarnych zawodach CTF uczestnik powinien zapoznać się z niniejszym Regulaminem dostępnym u koordynatorów uczelnianych Projektu oraz na stronie internetowej www.ecsc.mil.pl.
 23. Udział w ogólnopolskich stacjonarnych zawodach CTF jest równoznaczny z akceptacją Regulaminu.
 24. Podczas ogólnopolskich stacjonarnych zawodów CTF członkowie zespołów otrzymają jednorazowe kody pozwalające na założenie konta na dedykowanej platformie i udział w rozwiązywaniu zadań konkursowych.
 25. Organizatorzy zapewnią uczestnikom dostęp do sieci komputerowej.
 26. Uczestnicy ogólnopolskich stacjonarnych zawodów CTF korzystają z własnych komputerów. Konieczne jest posiadanie w komputerze przenośnym (notebooku) karty sieciowej, Ethernet, 100/1000Mbit/s ze złączem RJ45 i ewentualnie w przypadku chęci skorzystania z dodatkowego monitora posiadania złącza HDMI. Preferowany system operacyjny komputerów to Kali Linux lub ewentualnie maszyna wirtualna z tym systemem.
 27. Organizatorzy zapewnią dostęp do platformy wymienionej w § 2 pkt 7 dla każdego członka zespołu.
 28. Momentem rozpoczęcia ogólnopolskich stacjonarnych zawodów CTF jest oficjalne przedstawienie treści zadań podczas otwarcia zawodów. Dopiero od tego momentu możliwe jest zapoznanie się przez zespoły z treścią zadań i rozpoczęcie ich rozwiązywania.
 29. Po zapoznaniu się z tematem zadań i ogłoszeniu otwarcia ogólnopolskich stacjonarnych zawodów CTF, każdy z uczestników otrzyma instrukcję wykonywania zadań wraz z ich punktacją. Zawody będą trwały maksymalnie 8 godzin.
 30. Organizatorzy zastrzegają sobie prawo modyfikacji zadań. Każdy zespół będzie powiadomiony o wprowadzonej modyfikacji w celu doprecyzowania lub naprawienia błędu w zadaniu poprzez platformę.
 31. Aby rozwiązać zadanie należy znaleźć ukrytą flagę - specjalny ciąg znaków udowadniający rozwiązanie zadania lub wykonać określone czynności zmierzające do udzielenia odpowiedzi na pytanie. Za zgłoszenie za pomocą platformy flagi lub odpowiedzi uczestnicy dostają punkty. Znalezienie i zgłoszenie flagi lub udzielenie odpowiedzi na pytanie jest celem każdego zadania.
 32. Organizatorzy zawodów zapewnią uczestnikom kanał komunikacyjny (np. czat) umożliwiający zgłaszanie problemów z platformą i zadaniami w czasie trwania ogólnopolskich stacjonarnych zawodów CTF.
 33. Uczestnicy CTF zobowiązują się wykonać zadania stanowiące przedmiot zawodów samodzielnie i bez pomocy z zewnątrz.
 34. Uczestnikom ogólnopolskich stacjonarnych zawodów CTF nie wolno, pod rygorem natychmiastowego wykluczenia z udziału w zawodach, podejmować prób uzyskania dostępu do treści zadania przed rozpoczęciem zawodów.
 35. Organizatorzy mają prawo wykluczyć zespół z ogólnopolskich stacjonarnych zawodów CTF, jeżeli stwierdzą złamanie postanowień Regulaminu lub przepisów prawa powszechnie obowiązującego np.: ataki na infrastrukturę teleinformatyczną, niszczenie infrastruktury, niszczenie zadań lub utrudnianie rozwiązywania ich przez uczestników innych zespołów.
 36. Organizatorzy ogólnopolskich stacjonarnych zawodów CTF określą skład trzyosobowej Komisji oceniającej zawody.

37. Komisja oceniająca ze swego grona wybierze przewodniczącego.
38. Komisja dokona oceny zadań realizowanych przez poszczególne Zespoły, z czego sporządzi protokół oraz ogłosi wyniki ogólnopolskich stacjonarnych zawodów CTF.
39. Zakres wiedzy uczestników ogólnopolskich stacjonarnych zawodów CTF nie podlega ocenie przez Komisję oceniającą.
40. Decyzja Komisji oceniającej jest ostateczna i nie podlega odwołaniu.
41. Wyznaczone przez Organizatorów osoby zapewnią doraźną pomoc techniczną podczas trwania ogólnopolskich stacjonarnych zawodów CTF (wsparcie techniczne oraz merytoryczne, bez podpowiedzi odnośnie sposobu rozwiązywania zadań - dla uczestników w zakresie platformy).
42. Studenci biorący udział w ogólnopolskich stacjonarnych zawodach CTF będą mieli zapewnione bezpłatne wyżywienie podczas trwania wydarzenia.
43. Za uczestnictwo w ogólnopolskich stacjonarnych zawodach CTF dla wszystkich uczestników przewidziane są pakiety startowe.
44. Rozstrzygnięcie ogólnopolskich stacjonarnych zawodów CTF nastąpi w dniu 6 maja 2026 r.
45. Wyłonienia zwycięzców ogólnopolskich stacjonarnych zawodów CTF dokona Zespół składający się z przedstawicieli DC oraz ECSC.
46. Dla laureatów ogólnopolskich stacjonarnych zawodów CTF przewidziane są dodatkowe wyróżnienia i nagrody.
47. Na zakończenie ogólnopolskich stacjonarnych zawodów CTF nastąpi uroczyste zakończenie Projektu z wręczeniem dyplomów i nagród.
48. Zwycięzcy ogólnopolskich stacjonarnych zawodów CTF zostaną powiadomieni o wynikach zawodów w formie ustnej.
49. Zespoły, które zajmą I, II i III miejsce w ogólnopolskich stacjonarnych zawodach CTF, otrzymają od Organizatorów bilety na Konferencję CyberEXPERT organizowaną przez ECSC w listopadzie 2026 roku.
50. Zwycięzcy ogólnopolskich stacjonarnych zawodów CTF otrzymają szczególną nagrodę w postaci pakietu przygotowanego przez Akademię Marynarki Wojennej im. Bohaterów Westerplatte z siedzibą w Gdyni obejmującego wizytę i zwiedzanie gmachu AMW, zwiedzanie Portu Wojennego w Gdyni oraz rejs łodzią motorową po Zatoce Gdańskiej.
51. Warunkiem wydania nagród jest obecność podczas ogłaszania wyników zawodów CTF. Brak obecności powoduje utratę nagrody.
52. Laureaci mają prawo do rezygnacji z przyjęcia nagrody.
53. Wydarzenia stanowiące nagrody, o których mowa w pkt 49-50, odbędą się w miejscu, czasie i na warunkach ustalonych przez Organizatorów.
54. Uczestnicy CTF są zobowiązani do zachowania w poufności treści zadań zawodów oraz informacji, wiedzy, danych, jak również dokumentów i ich projektów udostępnionych przez Organizatorów lub opracowanych i/lub przygotowanych przez uczestników ogólnopolskich stacjonarnych zawodów CTF.
55. W celu uniknięcia jakichkolwiek wątpliwości Organizatorzy informują, że użyte w Regulaminie określenie *Informacje chronione* nie dotyczy informacji niejawnych w rozumieniu *Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (tj. Dz. U. z 2019 poz. 412 ze zm.)*.
56. Informacje chronione to treści zadań zawodów, informacje, wiedza, dane, jak również dokumenty i projekty dokumentów (także w postaci nieukończonej) udostępnione przez Organizatorów lub opracowane/przygotowane przez uczestników ogólnopolskich stacjonarnych zawodów CTF

w czasie ich trwania oraz 12 miesięcy po ich zakończeniu. To również informacje o charakterze technicznym, technologicznym (w tym dokumenty, oprogramowanie, dane), lub inne informacje uzyskane w wyniku analizy, lub przetworzenia dostarczonych informacji (w tym danych osobowych) oraz które:

- 1) nie zostały podane do publicznej wiadomości;
 - 2) które uczestnicy ogólnopolskich stacjonarnych zawodów CTF uzyskali i/lub które mogą stać się im znane w toku rozmów i/lub w związku z wykonywaniem przez uczestników zawodów.
57. Informacje chronione będą wykorzystywane przez uczestnika ogólnopolskich stacjonarnych zawodów CTF wyłącznie w celu udziału w zawodach.
58. Organizatorzy informują, że zobowiązanie do zachowania w poufności Informacji chronionych obejmuje m.in.:
- 1) zakaz rozpowszechniania, kopiowania lub dystrybucji, ujawniania, przekazywania, potwierdzania i/lub składania komentarzy dotyczących Informacji chronionych wobec osób i podmiotów trzecich i/lub nieupoważnionych osób, pośrednio bądź bezpośrednio;
 - 2) obowiązek niezwłocznego poinformowania Organizatorów o fakcie utraty, ujawnienia lub powielenia Informacji chronionej i/lub niedotrzymania warunków Regulaminu.
59. Uczestnik ogólnopolskich stacjonarnych zawodów CTF zobowiązuje się zwrócić Organizatorom wszelkie urządzenia, dokumenty (włączając ich kopie) oraz nośniki danych niezwłocznie po ich wykorzystaniu lub użyciu dla realizacji zawodów, oraz usunąć dane i informacje zapisane w pamięci komputera lub na innych nośnikach danych.
60. Organizatorzy zastrzegają sobie prawo odwołania lub ogólnopolskich stacjonarnych zawodów CTF przed czasem bez podania przyczyny.
61. Organizatorzy zastrzegają sobie prawo do dokonania zmian w Regulaminie bez konsultacji z uczestnikami ogólnopolskich stacjonarnych zawodów CTF.

§ 4. Ochrona danych osobowych

1. Administratorem danych osobowych uczestników biorących udział w Projekcie Akademia_CYBER.MIL w rozumieniu art. 13 *Rozporządzenia Parlamentu Europejskiego i Rady (DE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* jest Minister Obrony Narodowej z siedzibą w Warszawie, przy al. Niepodległości 218.
2. Klauzula informacyjna RODO stosowana przy Projekcie Akademia_CYBER.MIL w roku akademickim 2024/2025 wobec koordynatorów oraz studentów uczelni biorących w nim udział stanowi Załącznik nr 2 do Regulaminu.

OŚWIADCZENIE

uczestnika ogólnopolskich stacjonarnych zawodów Capture The Flag

Ja (imię i nazwisko)

Student (nazwa uczelni)

na kierunku

oświadczam, iż:

1. Jestem pełnoletnia/ni i posiadam pełną zdolność do czynności prawnych.
2. Posiadam obywatelstwo polskie.
3. Akceptuję zapisy Regulaminu Projektu Akademia_CYBER.MIL oraz zobowiązuję się do ich przestrzegania.
4. Zobowiązuję się do zachowania poufności w zakresie określonym w Regulaminie.

.....
(podpis studenta)

5. Wyrażam zgodę na dokumentowanie i utrwalanie wybranych przez Organizatorów zdarzeń w ramach ogólnopolskich stacjonarnych zawodów CTF, włącznie z rejestrowaniem dźwięku i obrazu, a w szczególności utrwalania mojego wizerunku w celu późniejszego wykorzystania tych materiałów do celów związanych z informowaniem przez Organizatorów o przebiegu zawodów i jego wyniku.

.....
(podpis studenta)

KLAUZULA INFORMACYJNA RODO

stosowana przy Projekcie Akademia_CYBER.MIL w roku akademickim 2025/2026
wobec koordynatorów oraz studentów uczelni biorących w nim udział

Działając na podstawie art. 14 ust. 1 i 2 RODO, informuję Panią/Pana, że: administratorem danych osobowych jest Minister Obrony Narodowej z siedzibą w Warszawie, przy al. Niepodległości 218, e-mail: dc.sekretariat@mon.gov.pl.

Administrator wyznaczył Inspektora Ochrony Danych, z którym można się kontaktować poprzez pocztę elektroniczną na adres: iod@mon.gov.pl lub listownie na adres: Ministerstwo Obrony Narodowej, al. Niepodległości 218, 00-911 Warszawa, z dopiskiem „Inspektor Ochrony Danych”.

Pani/Pana dane osobowe, tj.: imię i nazwisko, nazwa uczelni, e-mail z domeną uczelni, numer telefonu kontaktowego nazwa kierunku studiów (w przypadku studentów) oraz rok studiów (w przypadku studentów), pozyskane zostały z Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa i przetwarzane będą w celu zrealizowania *Decyzji Nr 304/DC Ministra Obrony Narodowej z dnia 8 września 2025 r. w sprawie realizacji Projektu Akademia_CYBER.MIL w roku akademickim 2025/2026*, która służy administratorowi do wykonania zadania realizowanego w interesie publicznym.

Podstawą prawną przetwarzania danych osobowych jest art. 6 ust. 1 lit. e RODO w związku z art. 2 pkt 1 i pkt 23 *ustawy z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej (Dz. U. z 2022 r. poz. 1438)*, § 2 pkt 3a *rozporządzenia Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. poz. 426 oraz z 2014 r. poz. 933)* oraz ww. *Decyzją Nr 304/DC Ministra Obrony Narodowej*, tj. przetwarzanie danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Dane osobowe będą przekazywane podmiotom przetwarzającym dane osobowe na zlecenie administratora, a także innym podmiotom uprawnionym na podstawie przepisów prawa, w tym podmiotowi współrealizującemu Projekt Akademia_CYBER.MIL, tj.: Wojskowemu Centrum Edukacji Obywatelskiej.

Dane nie będą przekazywane do państwa trzeciego ani do organizacji międzynarodowej.

Dane będą przechowywane przez okres 10 lat wynikający z przepisów prawa, tj. zgodnie z obowiązującym w Ministerstwie Obrony Narodowej „Jednolitym Rzeczowym Wykazem Akt”.

Osobie, której dane dotyczą, przysługuje prawo do:

- dostępu do danych osobowych; żądania ich sprostowania; ograniczenia przetwarzania, w przypadkach wymienionych w RODO,
- wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Osobie, której dane dotyczą, nie przysługuje prawo do: przenoszenia danych, usunięcia danych, wniesienia sprzeciwu.

Informuję, że prawo do sprzeciwu nie przysługuje Pani/Panu ze względu na to, że istnieją ważne, prawnie uzasadnione podstawy do przetwarzania Pani/Panu danych.

W trakcie przetwarzania danych nie będzie dochodziło do zautomatyzowanego podejmowania decyzji ani do profilowania.

**KLAUZULA INFORMACYJNA
DO PROJEKTU Akademia_CYBER.MIL**

Zgodnie z art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L Nr 119, s.1), zwanego dalej „RODO”, informujemy, że:

Administrator Danych Osobowych	Dyrektor Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa zwanego dalej „ECSC” z siedzibą w Warszawie pod adresem: ul. gen. Sylwestra Kaliskiego 2 00-908 Warszawa; tel.: 261-837-990 mail: sekretariat.ecsc@mon.gov.pl
Inspektor Ochrony Danych	Anna RUSINIAK tel: 261-837-990 Mail: ecsc.iod@mon.gov.pl
Cel przetwarzania danych osobowych	Przetwarzamy dane osobowe w związku realizacją Projektu Akademia_CYBER.MIL.
Podstawa prawna przetwarzania danych osobowych	Dane osobowe przetwarzane będą związku z obsługą korespondencji na podstawie art. 6 ust. 1 lit. c RODO, tj. przetwarzanie danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
Udostępnianie danych osobowych	Dane osobowe mogą być udostępniane podmiotom do tego uprawnionym na podstawie powszechnie obowiązujących przepisów prawa.
Przekazywanie danych poza Europejski Obszar Gospodarczy (EOG)	Dane nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.
Okres przetwarzania	Dane osobowe będą przechowywane do chwili zakończenia sprawy, w której zostały one zebrane, a następnie – w przypadkach, w których wymagają tego przepisy ustawy z dnia 14 lipca 1986 r. o narodowym zasobie archiwalnym i archiwach – przez czas określony w tych przepisach.
Twoje prawa	1) Przysługuje Państwu prawo do żądania od administratora dostępu do swoich danych osobowych, a także ich sprostowania, usunięcia, ograniczenia przetwarzania a także wniesienia sprzeciwu w związku z ich przetwarzaniem. 2) Na Państwa żądanie, ECSC wyda kopię danych osobowych.
Organ nadzorczy	Przysługuje Państwu prawo do złożenia skargi w związku z przetwarzaniem danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych.
Dobrowolność	Podanie danych osobowych jest dobrowolne ale niezbędne do korzystania z kursów e-learningowych w związku Z Decyzją Nr 304/DC Ministra Obrony Narodowej z dnia 8 września 2025 r. w sprawie realizacji Projektu Akademia_CYBER.MIL w roku

akademickim 2025/2026. Może Pan/Pani wycofać zgodę w dowolnym momencie wysyłając prośbę na adres Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa, co nie wpływa na zgodność z prawem przetwarzania, dokonanego przed jej cofnięciem.

Profilowanie

Dane osobowe nie będą poddane zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.