

REGULAMIN REKRUTACJI I UCZESTNICTWA W FORMACH WSPARCIA W POSTACI SZKOLEŃ SPECJALISTYCZNYCH REALIZOWANYCH W RAMACH PROJEKTU

„Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”

realizowanym przez **Politechnikę Śląską** w ramach zadania zleconego przez **Ministra Nauki i Szkolnictwa Wyższego**

Numer umowy z MNiSW: MNiSW/2026/DIR/253 z dnia 29.05.2026 r.

§ 1. Postanowienia ogólne

1. Niniejszy Regulamin określa zasady rekrutacji, kwalifikacji, uczestnictwa, ukończenia oraz dokumentowania udziału Uczestników w formach wsparcia w postaci szkoleń specjalistycznych realizowanych w ramach projektu pn. „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”, zwanego dalej „Projektem”.
2. Projekt jest realizowany przez Politechnikę Śląską, z siedzibą przy ul. Akademickiej 2A, 44-100 Gliwice, zwaną dalej „Organizatorem” albo „Uczelnią”, w ramach zadania zleconego przez Ministra Nauki i Szkolnictwa Wyższego, na podstawie umowy nr MNiSW/2026/DIR/253 z dnia 29 maja 2026 r.
3. Projekt ma charakter ogólnosektorowy i jest skierowany do podmiotów systemu szkolnictwa wyższego i nauki, w szczególności uczelni, instytutów badawczych, instytutów naukowych PAN oraz podmiotów działających w ramach Sieci Badawczej Łukasiewicz.
4. Udział w formach wsparcia objętych Projektem jest bezpłatny dla Uczestników, z zastrzeżeniem obowiązków wynikających z niniejszego Regulaminu i dokumentów rekrutacyjnych.
5. Projekt jest realizowany w terminie od dnia zawarcia umowy z Ministrem Nauki i Szkolnictwa Wyższego do dnia 31 grudnia 2026 r., przy czym dostęp do wybranych

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

- materiałów e-learningowych może być utrzymywany po zakończeniu Projektu, jeżeli wynika to z umowy, harmonogramu, trwałości rezultatów albo decyzji Organizatora.
6. Regulamin stosuje się łącznie z umową dotyczącą realizacji Zadania, opisem Zadania, kosztorysem, dokumentami wewnętrznymi Politechniki Śląskiej oraz przepisami prawa powszechnie obowiązującego.
 7. W sprawach organizacyjnych dotyczących rekrutacji i udziału w Szkoleniu właściwe jest Biuro Projektu: Politechnika Śląska, Wydział Automatyki, Elektroniki i Informatyki, ul. Akademicka 16, pok. 408, 44-100 Gliwice, e-mail: cyberedu@polsl.pl, tel. +48 32 237 13 39.
 8. Regulamin jest jednym z dokumentów stosowanych przy realizacji Projektu w zakresie rekrutacji i uczestnictwa. Regulamin stosuje się łącznie z dokumentami rekrutacyjnymi, komunikatami rekrutacyjnymi, programami szkoleń oraz właściwymi procedurami Politechniki Śląskiej, w zakresie, w jakim mają one zastosowanie do udziału Uczestników w Projekcie.

§ 2. Podstawy prawne i dokumenty stosowane przy realizacji Projektu

1. Rekrutacja i udział w formach wsparcia realizowanych w ramach Projektu odbywają się z uwzględnieniem w szczególności:
 1. umowy zawartej pomiędzy Ministrem Nauki i Szkolnictwa Wyższego a Politechniką Śląską wraz z opisem Zadania;
 2. ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce;;
 3. ustawy z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami;
 4. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.;
 5. ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
 6. Polityki ochrony danych osobowych na Politechnice Śląskiej;
 7. przepisów dotyczących obowiązków informacyjnych związanych z finansowaniem zadań ze środków publicznych;
 8. niniejszego Regulaminu, dokumentów rekrutacyjnych, programów Szkolenia oraz komunikatów Organizatora.
2. W przypadku sprzeczności Regulaminu z przepisami prawa powszechnie obowiązującego, umową zawartą z Ministrem albo obowiązującymi aktami wewnętrznymi Politechniki Śląskiej, pierwszeństwo mają odpowiednio: przepisy

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

prawa, umowa, akty wewnętrzne Politechniki Śląskiej, a następnie niniejszy Regulamin.

§ 3. Definicje

Na potrzeby Regulaminu przyjmuje się następujące definicje:

1. **Projekt** – zadanie pn. „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.
2. **Organizator / Uczelnia** – Politechnika Śląska z siedzibą w Gliwicach.
3. **Minister** – Minister Nauki i Szkolnictwa Wyższego albo właściwa komórka Ministerstwa obsługująca umowę.
4. **Biuro Projektu** – miejsce obsługi administracyjno-organizacyjnej rekrutacji i udziału w Projekcie, zlokalizowane pod adresem: Politechnika Śląska, Wydział Automatyki, Elektroniki i Informatyki, ul. Akademicka 16, 44-100 Gliwice, pok. 408, prowadzące kontakt z Kandydatami i Uczestnikami za pośrednictwem adresu e-mail: cyberedu@polsl.pl oraz telefonu: +48 32 237 13 39.
5. **Szkolenia** – szkolenia specjalistyczne będące jedną z form wsparcia realizowaną w ramach Projektu.
6. **Kandydat** – osoba, która zgłasza chęć udziału w Projekcie poprzez złożenie formularza zgłoszeniowego albo osoba zgłoszona przez instytucję delegującą, przed zakończeniem procedury kwalifikacyjnej.
7. **Uczestnik** – osoba zakwalifikowana do udziału w Projekcie, która złożyła wymagane dokumenty i została wpisana na listę Uczestników.
8. **Instytucja delegująca** – uczelnia, instytut badawczy, instytut naukowy PAN, podmiot Sieci Badawczej Łukasiewicz albo inny podmiot systemu szkolnictwa wyższego i nauki, który deleguje Kandydata na Szkolenia.
9. **Komisja Rekrutacyjna** – zespół co najmniej trzech osób powołany w trybie obowiązującym w Politechnice Śląskiej, odpowiedzialny za ocenę formalną zgłoszeń, kwalifikację Kandydatów, utworzenie listy podstawowej i listy rezerwowej oraz dokumentowanie przebiegu rekrutacji. Przewodniczącym Komisji Rekrutacyjnej jest Kierownik Projektu.
10. **Kierownik Projektu** – osoba odpowiedzialna za koordynację realizacji Projektu, przewodniczenie Komisji Rekrutacyjnej oraz podejmowanie decyzji organizacyjnych dotyczących udziału w Szkoleniu, w zakresie niezastrzeżonym dla Komisji Rekrutacyjnej.

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

11. **Platforma** – system teleinformatyczny wykorzystywany w Projekcie do komunikacji z Uczestnikami, udostępniania materiałów szkoleniowych, realizacji e-learningu, VoD, testów, egzaminów, ankiet ewaluacyjnych lub potwierdzania aktywności Uczestników. Dostęp do Platformy realizowany jest za pośrednictwem strony **cyberedu.polsl.pl**.
12. **Nagranie Szkolenia** – utrwalony w formie audiowizualnej albo dźwiękowej zapis przebiegu zajęć realizowanych w ramach Szkolenia, obejmujący w szczególności wypowiedzi, pytania, dyskusje, obraz lub głos Uczestników w zakresie wynikającym z formy prowadzenia zajęć. Nagranie jest wykorzystywane wyłącznie w zakresie wskazanym w Regulaminie, komunikacie rekrutacyjnym oraz klauzuli informacyjnej RODO.
13. **Dane osobowe** – dane osobowe w rozumieniu RODO, przetwarzane w zakresie niezbędnym do realizacji Projektu.

§ 4. Cel Projektu i zakres wsparcia w ramach Szkolenia

1. Celem Projektu jest zwiększenie poziomu wiedzy oraz praktycznych kompetencji z zakresu cyberbezpieczeństwa wśród osób związanych z podmiotami systemu szkolnictwa wyższego i nauki, w szczególności osób odpowiedzialnych za cyberbezpieczeństwo, kadry zarządczej oraz osób korzystających z materiałów z zakresu cyberhigieny.
2. Jednym z elementów Projektu jest przeprowadzenie badań dotyczących wpływu nowych podwyższonych wymagań w zakresie cyberbezpieczeństwa wynikających z implementacji dyrektywy NIS2 oraz nowelizacji przepisów dotyczących krajowego systemu cyberbezpieczeństwa (KSC) na zagadnienia związane z architekturą, zarządzaniem, zgodnością z prawem, ochroną infrastruktury, bezpieczeństwem systemów, monitorowaniem zdarzeń, zarządzaniem ryzykiem i innymi aspektami związanymi z cyberbezpieczeństwem. Wyniki badań przedstawione zostaną podczas specjalistycznego szkolenia z zakresu wdrażania zasad cyberbezpieczeństwa w podmiotach systemu szkolnictwa wyższego i nauki, obejmującego część wspólną realizowaną stacjonarnie oraz ścieżkę specjalistyczną w formule e-learningowej, VoD albo mieszanej, zwanego dalej Szkoleniem;
3. Weryfikacja udziału, dokumentowanie realizacji Szkolenia oraz potwierdzanie ukończenia Szkolenia będzie realizowane przez listy obecności, testy, zadania, ankiety ewaluacyjne oraz świadectwa ukończenia.
4. Szczegółowy program Szkolenia, harmonogram, liczba godzin, miejsce, tryb realizacji, liczba miejsc i zasady zaliczenia poszczególnych form wsparcia są ogłaszane przez

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

Organizatora w komunikacie rekrutacyjnym publikowanym na stronie internetowej Projektu: **cyberedu.polsl.pl** lub przekazywanym Kandydatom i Uczestnikom za pośrednictwem poczty elektronicznej albo Platformy.

5. Organizator może zmienić harmonogram, miejsce albo formę zajęć, jeżeli jest to uzasadnione względami organizacyjnymi, bezpieczeństwa, dostępności, liczbą zgłoszeń, dostępnością prowadzących albo innymi okolicznościami wpływającymi na prawidłową realizację Szkolenia.

§ 5. Grupa docelowa i warunki udziału w Szkoleniu

1. Do udziału w Szkoleniu mogą zostać zakwalifikowane osoby, które należą do grupy docelowej i spełniają kryteria formalne określone w komunikacie rekrutacyjnym.
2. Grupę docelową stanowią osoby odpowiedzialne lub przewidziane do odpowiedzialności za cyberbezpieczeństwo w podmiotach systemu szkolnictwa wyższego i nauki, w tym pełnomocnicy, koordynatorzy, CISO, pracownicy IT, osoby odpowiedzialne za bezpieczeństwo informacji, ciągłość działania, zarządzanie ryzykiem, audyt bezpieczeństwa, obsługę incydentów albo SZBI;
3. Warunkiem udziału jest złożenie formularza zgłoszeniowego oraz wymaganej dokumentacji określonej w § 6, w tym potwierdzenia delegowania Kandydata przez instytucję delegującą, zgodnie ze wzorem stanowiącym Załącznik nr 3 do Regulaminu. Potwierdzenie delegowania jest wymagane od każdego Kandydata zgłaszanego do tej formy wsparcia. Potwierdzenie może zostać podpisane przez osobę upoważnioną do reprezentowania instytucji albo przez osobę upoważnioną do delegowania pracownika do udziału w szkoleniu, w szczególności rektora, prorektora, dyrektora instytutu, kanclerza, kierownika jednostki organizacyjnej, bezpośredniego przełożonego albo inną osobę wskazaną przez instytucję.
4. Warunkiem udziału w Szkoleniu jest przyjęcie przez Kandydata do wiadomości, że Szkolenie jest realizowane w formule nagrywanej, a nagranie może obejmować jego wizerunek, głos, wypowiedzi, pytania, udział w dyskusji, nazwę wyświetlaną na Platformie albo inne dane ujawnione podczas zajęć.
5. Kandydat, który nie akceptuje udziału w Szkoleniu prowadzonym w formule nagrywanej, nie może zostać zakwalifikowany do tej edycji Szkolenia. Powyższe nie dotyczy odrębnej, fakultatywnej zgody na publiczne wykorzystanie wizerunku lub głosu w celach promocyjnych.

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

6. Organizator zapewnia, że nagrania Szkolenia nie będą publikowane publicznie ani wykorzystywane w celach promocyjnych wyłącznie na podstawie akceptacji, o której mowa w ust. 4.
7. Instytucja delegująca może delegować więcej niż jednego Kandydata poprzez potwierdzenie delegowania zgodnie ze wzorem stanowiącym Załącznik nr 3 do Regulaminu.
8. Zgłoszenie Kandydata nie jest równoznaczne z zakwalifikowaniem do Szkolenia.

§ 6. Rekrutacja

1. Rekrutacja jest prowadzona w sposób transparentny, z poszanowaniem zasad równego traktowania, niedyskryminacji, dostępności dla osób ze szczególnymi potrzebami oraz adekwatności danych osobowych.
2. Rekrutacja może być prowadzona w trybie ciągłym albo w turach, do wyczerpania limitu miejsc, środków finansowych albo terminu wynikającego z harmonogramu Projektu.
3. Informacja o naborze zawiera co najmniej: nazwę Projektu, nazwę Organizatora, źródło finansowania, grupę docelową, liczbę miejsc, termin i sposób zgłoszeń, kryteria kwalifikacji, zakres wymaganych dokumentów, informację o dostępności oraz dane kontaktowe Biura Projektu.
4. Procedura rekrutacji składa się z kolejnych etapów:
 1. Ogłoszenie naboru na stronie internetowej Projektu: cyberedu.polsl.pl oraz równoczesne rozpowszechnienie informacji o naborze za pośrednictwem wybranych kanałów komunikacji, w szczególności strony internetowej Politechniki Śląskiej, wiadomości e-mail kierowanej do podmiotów systemu szkolnictwa wyższego i nauki, komunikacji za pośrednictwem partnerów organizacyjnych Projektu, oficjalnych kanałów informacyjnych Politechniki Śląskiej oraz mediów społecznościowych Politechniki Śląskiej.
 2. Złożenie zgłoszeń przez Kandydatów składających się z:
 1. Wypełnionego formularza zgłoszeniowego Kandydata, stanowiącego Załącznik nr 1 do Regulaminu. Formularz może zostać wypełniony elektronicznie na stronie cyberedu.polsl.pl lub papierowo po skontaktowaniu się z Biurem Projektu. Osoba, która potrzebuje formularza w innej dostępnej formie lub pomocy w jego wypełnieniu albo innego usprawnienia, może skontaktować się z Biurem Projektu. Zgłoszenie potrzeby dostępności nie wpływa negatywnie na ocenę

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

- zgłoszenia i służy wyłącznie umożliwieniu udziału w Projekcie na zasadach równego dostępu.
2. Potwierdzenia delegowania przez instytucję, stanowiącego Załącznik nr 3 do Regulaminu. W przypadku zgłoszenia za pomocą formularza elektronicznego, Kandydat powinien załadować w serwisie w kursie „Sprawy Ogólne” dokument podpisany cyfrowo lub skan – w tym drugim przypadku w razie zakwalifikowania Kandydata konieczne będzie dostarczenie oryginału dokumentu do Biura Projektu.
 3. Potwierdzenia zapoznania się z klauzulą informacyjną RODO, stanowiącą Załącznik nr 4 do Regulaminu.
 4. Informacji o potrzebach dostępności albo wniosku o zapewnienie dostępności, stanowiącego Załącznik nr 5 do Regulaminu - jeżeli Kandydat zgłasza takie potrzeby.
 5. Potwierdzenia przez Kandydata zapoznania się z zasadami nagrywania Szkolenia oraz przyjęcia nagrywanego trybu realizacji zajęć, zgodnie z oświadczeniem zawartym w formularzu zgłoszeniowym.
 3. Ocena formalna zgłoszenia, w tym weryfikacja kompletności dokumentów i przynależności do grupy docelowej.
 4. Podjęcie przez Komisję Rekrutacyjną decyzji o zakwalifikowaniu, niezakwalifikowaniu albo wpisaniu Kandydata na listę rezerwową, jeżeli liczba zgłoszeń przekracza liczbę miejsc, zgodnie z kryteriami określonymi w § 7.
 5. Poinformowanie Kandydata o wyniku rekrutacji indywidualnie, za pośrednictwem poczty elektronicznej, Platformy albo telefonicznie, jeżeli Kandydat wskazał telefon jako preferowany kanał kontaktu w sprawach dostępności.
 6. Przekazanie przez Kandydata zakwalifikowanego do udziału w Szkoleniu Deklaracji uczestnictwa stanowiącej Załącznik nr 2 do Regulaminu, w terminie wskazanym przez Organizatora.
 7. Załącznik nr 2 jest składany wyłącznie przez Kandydatów zakwalifikowanych do udziału w Szkoleniu. Od Kandydatów niezakwalifikowanych oraz wpisanych wyłącznie na listę rezerwową Organizator nie wymaga złożenia Deklaracji uczestnictwa.
 5. Organizator nie publikuje imiennych list Kandydatów zakwalifikowanych, niezakwalifikowanych ani wpisanych na listę rezerwową. Informacja o wyniku rekrutacji jest przekazywana Kandydatom indywidualnie.
 6. W przypadku braków formalnych Organizator może wezwać Kandydata do ich uzupełnienia w wyznaczonym terminie. Brak uzupełnienia dokumentów może skutkować pozostawieniem zgłoszenia bez rozpoznania.

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

7. Kwalifikacja do udziału następuje do wyczerpania limitu miejsc. W przypadku wolnych miejsc Organizator może prowadzić dodatkowy nabór albo kwalifikować osoby z listy rezerwowej.
8. Kandydat jest zobowiązany podać prawdziwe dane. Organizator może odmówić udziału albo skreślić Uczestnika z listy, jeżeli zgłoszenie zawiera dane nieprawdziwe, niepełne albo wprowadzające w błąd.

§ 7. Kryteria kwalifikacji i lista rezerwowa

1. Kwalifikacji Kandydatów dokonuje Komisja Rekrutacyjna pod przewodnictwem Kierownika Projektu, w oparciu o kryteria formalne i kryteria pierwszeństwa określone w Regulaminie.
 1. Komisja Rekrutacyjna sporządza protokół z przebiegu kwalifikacji, zawierający w szczególności liczbę zgłoszeń, wyniki oceny formalnej, listę osób zakwalifikowanych i listę rezerwową. Członek Komisji Rekrutacyjnej, wobec którego zachodzi konflikt interesów dotyczący danego Kandydata, nie bierze udziału w ocenie tego zgłoszenia.
2. Kryteriami formalnymi są:
 1. przynależność Kandydata do grupy docelowej określonej w § 5 ust. 2;
 2. złożenie kompletnego formularza zgłoszeniowego wraz z wymaganymi dokumentami określonymi w § 6;
 3. akceptacja Regulaminu oraz potwierdzenie zapoznania się z klauzulą informacyjną dotyczącą przetwarzania danych osobowych;
 4. wskazanie instytucji delegującej oraz statusu uzasadniającego udział w Szkoleniu;
 5. złożenie oświadczenia o możliwości uczestnictwa w Szkoleniu zgodnie z jego harmonogramem oraz spełnienia warunków ukończenia Szkolenia określonych w Regulaminie.
3. Jeżeli liczba kompletnych zgłoszeń przekracza liczbę miejsc, Kandydaci są kwalifikowani według kolejności wpływu kompletnego zgłoszenia, z zastrzeżeniem, że w pierwszej kolejności z jednej instytucji delegującej może zostać zakwalifikowanych maksymalnie dwóch Kandydatów w ramach danej tury rekrutacji oraz pierwszeństwo mają Kandydaci reprezentujący uczelnie publiczne.
4. Za kompletne zgłoszenie uważa się formularz zgłoszeniowy wraz z wymaganym potwierdzeniem delegowania oraz dokumentami wskazanymi w § 6.

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

5. Po zakwalifikowaniu maksymalnie dwóch Kandydatów z danej instytucji kolejne osoby z tej instytucji wpisuje się na listę rezerwową. Jeżeli po zakończeniu pierwszego etapu kwalifikacji pozostaną wolne miejsca, Komisja Rekrutacyjna może zakwalifikować kolejne osoby z instytucji już reprezentowanych, według kolejności wpływu kompletnych zgłoszeń.
6. Informacja o wyniku rekrutacji jest przekazywana Kandydatowi indywidualnie co najmniej jednym z następujących kanałów: pocztą elektroniczną, przez Platformę, telefonicznie albo w formie pisemnej. Jeżeli Kandydat zgłosił potrzebę dostępności dotyczącą sposobu komunikacji, Organizator stosuje wskazany dostępny kanał komunikacji, o ile jest to technicznie i organizacyjnie możliwe.
7. Kandydat może zwrócić się o ponowne sprawdzenie wyniku rekrutacji wyłącznie w zakresie błędu formalnego, w terminie 3 dni roboczych od otrzymania informacji o wyniku.

§ 8. Dokumenty rekrutacyjne i komunikacja z Uczestnikiem

1. Dokumentami rekrutacyjnymi i uczestnictwa są:
 1. Załącznik nr 1 - Formularz zgłoszeniowy Kandydata;
 2. Załącznik nr 2 – Deklaracja uczestnictwa i akceptacja Regulaminu, składana wyłącznie przez Kandydata zakwalifikowanego do udziału w Szkoleniu;
 3. Załącznik nr 3 - Potwierdzenie delegowania przez instytucję;
 4. Załącznik nr 4 - Klauzula informacyjna RODO dla Kandydatów i Uczestników;
 5. Załącznik nr 5 – Wniosek o zapewnienie dostępności, składany wyłącznie przez Kandydata albo Uczestnika zgłaszającego potrzebę zapewnienia dostępności lub racjonalnego usprawnienia;
 6. Załącznik nr 6 - Dobrowolna zgoda na wykorzystanie wizerunku i głosu w materiałach promocyjnych - składana wyłącznie w przypadku wyrażenia zgody przez Kandydata albo Uczestnika;
 7. Załącznik nr 7 - Oświadczenie o rezygnacji z udziału w Projekcie - składane w przypadku rezygnacji z udziału.
2. Dokumenty rekrutacyjne mogą być składane:
 1. elektronicznie - poprzez formularz internetowy albo Platformę;
 2. elektronicznie - jako dokument podpisany kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym przesłany na adres mailowy Biura Projektu;

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

3. papierowo - przez złożenie podpisanego formularza w Biurze Projektu albo przesłanie go na adres Biura Projektu.
3. W przypadku zgłoszenia elektronicznego Kandydat może załączyć skan podpisanego potwierdzenia delegowania. Kwalifikacja Kandydata dokonana na podstawie skanu ma charakter warunkowy.
4. Kandydat zakwalifikowany warunkowo jest zobowiązany, w terminie wskazanym przez Organizatora, przedstawić oryginał potwierdzenia delegowania w formie papierowej albo przekazać dokument elektroniczny podpisany kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.
5. Niedostarczenie lub nieprzekazanie dokumentu w terminie powoduje utratę miejsca w Szkoleniu, a Komisja Rekrutacyjna może zakwalifikować osobę z listy rezerwowej.
6. Podstawową formą komunikacji z Kandydatami i Uczestnikami jest poczta elektroniczna oraz Platforma. W sprawach dotyczących dostępności Organizator zapewnia również możliwość kontaktu telefonicznego albo korespondencyjnego. Kandydat i Uczestnik są zobowiązani do bieżącego sprawdzania korespondencji oraz aktualizowania danych kontaktowych.
7. Dokumenty rekrutacyjne i projektowe nie podlegają zwrotowi, chyba że przepisy prawa, decyzja Organizatora albo odrębna procedura stanowią inaczej.

§ 9. Organizacja zajęć i korzystanie z Platformy

1. Zajęcia mogą być realizowane stacjonarnie, online, w formule e-learningowej, w formule VoD albo w formule mieszanej.
 1. Szkolenie jest nagrywane w całości w formie audiowizualnej albo dźwiękowej, w zakresie obejmującym przebieg zajęć, prezentacje, wypowiedzi prowadzących, pytania, dyskusje oraz wypowiedzi Uczestników.
 2. Nagranie może obejmować wizerunek, głos, nazwę wyświetlaną na Platformie, wypowiedzi oraz inne dane osobowe ujawnione przez Uczestnika podczas Szkolenia. Uczestnik powinien ograniczać zakres ujawnianych danych do informacji niezbędnych dla udziału w zajęciach.
 3. Nagranie jest wykorzystywane wyłącznie do realizacji Szkolenia, w szczególności do umożliwienia odtworzenia zajęć przez Uczestników danej edycji, zapewnienia ciągłości procesu dydaktycznego, dokumentowania realizacji Szkolenia, kontroli jakości, rozliczenia Projektu oraz realizacji obowiązków wobec podmiotów uprawnionych do kontroli.

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

4. Dostęp do nagrań mają wyłącznie Uczestnicy danej edycji Szkolenia, prowadzący zajęcia, Kierownik Projektu, upoważnieni członkowie zespołu projektowego, administratorzy techniczni Platformy oraz podmioty uprawnione do kontroli lub audytu Projektu – wyłącznie w zakresie niezbędnym do realizacji ich zadań.
5. Nagrania są przechowywane do końca okresu dostępu do materiałów danej edycji Szkolenia, określonego w komunikacie rekrutacyjnym, a następnie usuwane albo poddawane anonimizacji, chyba że ich dalsze przechowywanie jest niezbędne z uwagi na obowiązek wynikający z przepisów prawa, umowy z Ministrem, kontroli, audytu albo dochodzenia lub obrony roszczeń.
6. Uczestnik nie może ujawniać podczas nagrywanego Szkolenia danych osobowych osób trzecich, informacji niejawnych, tajemnic prawnie chronionych, danych dotyczących realnych incydentów, podatności, konfiguracji infrastruktury ani innych informacji poufnych, chyba że zostało to uprzednio wyraźnie dopuszczone przez Organizatora i jest zgodne z przepisami prawa.
2. Uczestnik otrzymuje dostęp do Platformy w zakresie i na okres niezbędny do realizacji danej formy wsparcia. Dostęp ma charakter imienny i nie może być udostępniany osobom trzecim.
3. Uczestnik jest zobowiązany korzystać z Platformy zgodnie z jej przeznaczeniem, Regulaminem, instrukcjami technicznymi, zasadami bezpieczeństwa informacji oraz dobrymi praktykami cyberbezpieczeństwa.
4. Uczestnik nie może wprowadzać do Platformy danych osobowych, tajemnic prawnie chronionych, informacji niejawnych, poufnych informacji instytucji delegującej ani innych danych wrażliwych, jeżeli nie jest to konieczne do udziału w szkoleniu albo nie zostało wyraźnie dopuszczone przez Organizatora.
5. Jeżeli w ramach szkolenia wykorzystywane jest narzędzie do samooceny zgodności z wymaganiami NIS2/KSC, Uczestnik korzysta z niego wyłącznie w celu edukacyjnym, szkoleniowym albo wewnętrznym instytucji delegującej. Wyniki samooceny nie stanowią audytu, opinii prawnej, certyfikacji ani wiążącego potwierdzenia zgodności instytucji z wymaganiami prawa.
6. Organizator może rejestrować obecność Uczestników, aktywność na Platformie, wyniki testów i egzaminów oraz inne dane wskaźnikowe niezbędne do realizacji, monitoringu, ewaluacji, kontroli i rozliczenia Projektu.
7. Korzystanie z Platformy, formularza rekrutacyjnego, systemu egzaminacyjnego, narzędzia e-learningowego, narzędzia AI albo innego systemu teleinformatycznego wykorzystywanego w Projekcie musi być zgodne z Polityką ochrony danych osobowych na Politechnice Śląskiej oraz właściwymi procedurami bezpieczeństwa

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

informacji. Jeżeli dane rozwiązanie jest obsługiwane przez podmiot zewnętrzny, wymagane jest uprzednie zapewnienie zgodności z RODO, w szczególności weryfikacja podmiotu przetwarzającego oraz zawarcie wymaganej umowy powierzenia przetwarzania danych osobowych albo innego właściwego porozumienia.

8. Dostęp do danych osobowych przetwarzanych w Projekcie mogą posiadać wyłącznie osoby upoważnione albo podmioty, którym dane udostępniono lub powierzono zgodnie z przepisami prawa i procedurami Politechniki Śląskiej.
9. W formularzach, na Platformie i w narzędziach szkoleniowych będą zbierane wyłącznie dane adekwatne, stosowne i ograniczone do tego, co niezbędne do realizacji celów Projektu.
10. W przypadku wystąpienia incydentu bezpieczeństwa informacji albo podejrzenia naruszenia ochrony danych osobowych osoby zaangażowane w realizację Projektu są zobowiązane niezwłocznie poinformować Kierownika Projektu lub zespół projektowy oraz postępować zgodnie z Polityką ochrony danych osobowych na Politechnice Śląskiej.

§ 10. Prawa Uczestnika

Uczestnik ma prawo do:

1. dobrowolnego i nieodpłatnego korzystania z form wsparcia, do których został zakwalifikowany;
2. udziału w formach wsparcia, do których został zakwalifikowany;
3. otrzymania informacji o programie, harmonogramie, miejscu, formie i zasadach zaliczenia;
4. korzystania z materiałów szkoleniowych w zakresie dopuszczonym przez Organizatora;
5. zgłoszenia potrzeb dostępności, w tym potrzeby zapewnienia racjonalnego usprawnienia albo dostępu alternatywnego;
6. zgłaszania uwag organizacyjnych, merytorycznych i technicznych do Biura Projektu;
7. otrzymania świadectwa ukończenia szkolenia, zaświadczenia albo innego dokumentu potwierdzającego udział lub ukończenie danej formy wsparcia, jeżeli spełni warunki ukończenia określone w Regulaminie, programie szkolenia albo komunikacie Organizatora;
8. ochrony danych osobowych zgodnie z RODO, ustawą o ochronie danych osobowych oraz Polityką ochrony danych osobowych na Politechnice Śląskiej.

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

§ 11. Obowiązki Uczestnika

1. Uczestnik jest zobowiązany do:

1. przestrzegania Regulaminu, komunikatów Organizatora oraz zasad obowiązujących w miejscu prowadzenia zajęć;
2. uczestnictwa w zajęciach w sposób aktywny, terminowy i systematyczny;
3. potwierdzania obecności w sposób wskazany przez Organizatora;
4. realizacji testów, egzaminów, ankiet, zadań problemowych lub innych form weryfikacji efektów uczenia się, jeżeli są przewidziane dla danej formy wsparcia;
5. korzystania z udostępnionych materiałów i dostępu do Platformy wyłącznie na potrzeby udziału w Projekcie albo w zakresie dopuszczonym przez Organizatora;
6. nieudostępniania osobom trzecim kont, haseł, linków dostępowych, testów, egzaminów, nagrań, materiałów szkoleniowych oraz innych zasobów Projektu, chyba że Organizator wyraźnie dopuści takie wykorzystanie;
7. nieutrwalania i nierozpowszechniania zajęć, wypowiedzi prowadzących, wypowiedzi innych Uczestników, wizerunku osób uczestniczących oraz materiałów projektowych bez zgody Organizatora i osób, których to dotyczy;
8. bieżącego informowania Kierownika Projektu, zespołu projektowego albo Biura Projektu o zmianie danych, braku możliwości udziału, rezygnacji, zdarzeniach losowych albo innych okolicznościach mogących wpływać na udział w Projekcie;
9. zachowania poufności informacji, które zostały oznaczone jako poufne albo których poufny charakter wynika z okoliczności, w szczególności informacji o incydentach, rozwiązaniach bezpieczeństwa, infrastrukturze IT, procedurach wewnętrznych lub dokumentacji SZBI instytucji delegujących;
10. niepodjęmowania działań mogących naruszać bezpieczeństwo Platformy, systemów Organizatora, prowadzących, innych Uczestników albo instytucji delegujących.
11. powstrzymywania się od ujawniania podczas nagrywanych zajęć danych osobowych osób trzecich, danych szczególnych kategorii, tajemnic prawnie chronionych, informacji niejawnych, danych o realnych incydentach, podatnościach, konfiguracji systemów, infrastrukturze IT albo innych informacji poufnych, jeżeli ich ujawnienie nie jest niezbędne i wyraźnie dopuszczone przez Organizatora.

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

2. W przypadku zajęć stacjonarnych Uczestnik jest zobowiązany przestrzegać zasad bezpieczeństwa, regulaminów obiektu, instrukcji porządkowych, zasad ochrony przeciwpożarowej oraz poleceń osób odpowiedzialnych za organizację wydarzenia.

§ 12. Warunki ukończenia szkolenia i zasady egzaminowania

1. Warunki ukończenia danej formy wsparcia są określone w programie szkolenia, komunikacie rekrutacyjnym albo na Platformie.
2. Co do zasady warunkiem ukończenia szkolenia specjalistycznego jest łączne spełnienie następujących wymagań:
 1. udział w wymaganej liczbie zajęć, nie mniejszej niż 80% godzin przewidzianych dla danej formy wsparcia, chyba że program szkolenia wskazuje inny próg;
 2. realizacja wymaganych aktywności e-learningowych albo VoD;
 3. zaliczenie testów, egzaminu końcowego, zadania problemowego albo innych form weryfikacji efektów uczenia się, jeżeli zostały przewidziane w programie szkolenia, komunikacie rekrutacyjnym albo informacji przekazanej Uczestnikom przed rozpoczęciem danej formy weryfikacji;
 4. wypełnienie wymaganych ankiet ewaluacyjnych i dokumentów projektowych;
 5. brak zaległości formalnych wobec Biura Projektu.
3. Egzaminy i testy mogą być prowadzone stacjonarnie, elektronicznie albo z wykorzystaniem Platformy. Organizator może stosować mechanizmy zapewniające samodzielność pracy, integralność wyników i identyfikację Uczestnika.
4. Uczestnik, który nie zaliczył egzaminu albo testu końcowego, może przystąpić do jednego terminu poprawkowego, chyba że Organizator w programie szkolenia przewidzi inne zasady.
5. Świadectwo ukończenia szkolenia, zaświadczenie albo inny dokument potwierdzający udział lub ukończenie danej formy wsparcia wydaje się wyłącznie osobom, które spełniły warunki ukończenia danej formy wsparcia.
6. Świadectwo ukończenia szkolenia wydawane przez Politechnikę Śląską potwierdza udział i zaliczenie formy wsparcia w ramach Projektu. Nie stanowi ono zewnętrznej certyfikacji zawodowej, uprawnienia regulowanego ani potwierdzenia zgodności instytucji z KSC/NIS2.
7. Ewentualna walidacja albo certyfikacja zewnętrzna może zostać przeprowadzona przez odrębny podmiot certyfikujący, poza zakresem niniejszego Regulaminu, na zasadach określonych przez ten podmiot oraz w odrębnym komunikacie Organizatora.

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

§ 13. Rezygnacja, nieobecności i skreślenie z listy Uczestników

1. Uczestnik może zrezygnować z udziału w Projekcie, składając pisemne albo elektroniczne oświadczenie o rezygnacji do Biura Projektu.
2. Rezygnacja powinna zostać zgłoszona niezwłocznie, nie później niż w terminie 3 dni roboczych od powzięcia informacji o okolicznościach uniemożliwiających udział. W miarę możliwości rezygnacja powinna nastąpić przed rozpoczęciem danej formy wsparcia, aby umożliwić udział osobie z listy rezerwowej.
3. Uczestnik może zostać skreślony z listy Uczestników w szczególności w przypadku:
 1. nieusprawiedliwionej nieobecności przekraczającej limit określony w programie szkolenia;
 2. braku realizacji aktywności wymaganych na Platformie;
 3. braku przystąpienia do egzaminu albo testu końcowego bez usprawiedliwienia;
 4. naruszenia Regulaminu, zasad bezpieczeństwa, zasad poufności lub zasad korzystania z Platformy;
 5. podania nieprawdziwych danych w zgłoszeniu albo dokumentacji projektowej;
 6. udostępnienia osobom trzecim materiałów, testów, nagrań, konta, hasła albo dostępu do Platformy;
 7. zachowania uniemożliwiającego prowadzenie zajęć albo naruszającego prawa innych Uczestników.
4. W przypadku rezygnacji albo skreślenia Uczestnika Organizator może zakwalifikować osobę z listy rezerwowej.
5. Jeżeli rezygnacja po rozpoczęciu szkolenia albo skreślenie z listy nastąpiły z przyczyn zawinionych przez Uczestnika i spowodowały powstanie rzeczywistych, udokumentowanych kosztów po stronie Organizatora, Organizator może podjąć działania przewidziane w dokumentach projektowych, odrębnej deklaracji uczestnictwa, umowie z instytucją delegującą albo przepisach prawa. Decyzja w tym zakresie jest podejmowana indywidualnie przez Kierownika Projektu, z uwzględnieniem zasady proporcjonalności i okoliczności sprawy.

§ 14. Dostępność, równe traktowanie i przeciwdziałanie dyskryminacji

1. Projekt jest realizowany z poszanowaniem zasad równego traktowania, niedyskryminacji oraz dostępności dla osób ze szczególnymi potrzebami.

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

2. Organizator zapewnia dostępność architektoniczną, cyfrową oraz informacyjno-komunikacyjną w zakresie Projektu co najmniej w zakresie minimalnych wymagań wynikających z przepisów prawa, a jeżeli nie jest to możliwe z przyczyn technicznych lub prawnych – zapewnia dostęp alternatywny.
3. Kandydat lub Uczestnik może zgłosić potrzeby dostępności na etapie rekrutacji albo niezwłocznie po ich powstaniu. Zgłoszenie powinno zawierać opis potrzeby oraz, jeżeli to możliwe, preferowany sposób zapewnienia dostępności.
4. Zgłoszenie potrzeb dostępności nie może stanowić podstawy odmowy udziału w Projekcie ani pogorszenia sytuacji Kandydata lub Uczestnika.
5. Materiały cyfrowe, formularze, komunikaty oraz treści e-learningowe będą przygotowywane z uwzględnieniem wymagań dostępności właściwych dla treści cyfrowych i materiałów edukacyjnych finansowanych ze środków publicznych.

§ 15. Ochrona danych osobowych

1. Administratorem danych osobowych Kandydatów i Uczestników jest Politechnika Śląska z siedzibą w Gliwicach przy ul. Akademickiej 2A, 44-100 Gliwice, reprezentowana przez Rektora.
2. Z Inspektorem Ochrony Danych można kontaktować się pod adresem e-mail: iod@polsl.pl albo pisemnie na adres Politechniki Śląskiej z dopiskiem „Inspektor Ochrony Danych”.
3. Dane osobowe są przetwarzane w celu przeprowadzenia rekrutacji, organizacji udziału w Projekcie, prowadzenia list obecności, komunikacji, obsługi Platformy, nagrywania zajęć, przechowywania i ograniczonego udostępniania nagrań Uczestnikom danej edycji Szkolenia, prowadzącym, zespołowi projektowemu oraz podmiotom uprawnionym do kontroli lub audytu, testów i egzaminów, wydania świadectw ukończenia, zaświadczeń albo innych dokumentów potwierdzających udział lub ukończenie szkolenia, monitoringu, ewaluacji, kontroli, sprawozdawczości, archiwizacji, realizacji obowiązków informacyjnych oraz rozliczenia zadania finansowanego ze środków publicznych.
4. Zakres przetwarzanych danych obejmuje dane niezbędne do realizacji Projektu, w szczególności: imię i nazwisko, dane kontaktowe, nazwę instytucji delegującej, stanowisko lub funkcję, status w grupie docelowej, informacje o potrzebach dostępności, dane dotyczące uczestnictwa, obecności, wyników testów i egzaminów, wydanych zaświadczeń, świadectw ukończenia albo innych dokumentów potwierdzających udział lub ukończenie szkolenia oraz dane wymagane do monitoringu i sprawozdawczości, dane utrwalone w nagraniach Szkolenia, w szczególności

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

- wizerunek, głos, wypowiedzi, pytania, nazwa wyświetlana na Platformie oraz dane ujawnione przez Uczestnika podczas zajęć.
5. Podstawą prawną przetwarzania danych jest w szczególności art. 6 ust. 1 lit. c RODO, art. 6 ust. 1 lit. e RODO, a w zakresie czynności opartych na dobrowolnej zgodzie – art. 6 ust. 1 lit. a RODO. Jeżeli przetwarzanie jest niezbędne do zawarcia albo wykonania umowy lub deklaracji uczestnictwa, podstawą może być również art. 6 ust. 1 lit. b RODO.
 6. Dane osobowe mogą być udostępniane lub powierzane, wyłącznie w zakresie niezbędnym do realizacji Projektu, następującym kategoriom odbiorców:
 1. Ministrowi Nauki i Szkolnictwa Wyższego oraz podmiotom uprawnionym do kontroli, audytu, nadzoru lub rozliczenia Projektu;
 2. osobom i jednostkom Politechniki Śląskiej zaangażowanym w realizację, obsługę, rozliczenie, archiwizację lub nadzór nad Projektem;
 3. prowadzącym zajęcia, członkom Komisji Rekrutacyjnej oraz osobom realizującym zadania egzaminacyjne, ewaluacyjne lub organizacyjne;
 4. Uczestnikom tej samej edycji Szkolenia - wyłącznie w zakresie dostępu do nagrań udostępnianych w zamkniętym środowisku technicznym;
 5. dostawcom i operatorom Platformy, systemów informatycznych, usług nagrywania, hostingu, poczty elektronicznej, narzędzi egzaminacyjnych lub e-learningowych - wyłącznie na zasadach zgodnych z RODO oraz procedurami Politechniki Śląskiej;
 6. podmiotom świadczącym na rzecz Politechniki Śląskiej usługi prawne, archiwizacyjne, techniczne, audytowe, księgowe lub organizacyjne;
 7. podmiotom certyfikującym lub walidującym - wyłącznie jeżeli Uczestnik przystępuje do zewnętrznej certyfikacji na zasadach określonych odrębnie przez Organizatora lub podmiot certyfikujący.
 7. Dane osobowe będą przechowywane przez okres realizacji Projektu oraz okres wymagany dla archiwizacji, kontroli i rozliczenia zadania, nie krócej niż przez okres przechowywania dokumentacji określony w umowie z Ministrem i przepisach prawa, z uwzględnieniem instrukcji kancelaryjnej i archiwalnej obowiązującej w Politechnice Śląskiej.
 8. Osobie, której dane dotyczą, przysługuje prawo dostępu do danych, sprostowania, ograniczenia przetwarzania, usunięcia danych w przypadkach przewidzianych prawem, wniesienia sprzeciwu, przenoszenia danych w przypadkach przewidzianych prawem, cofnięcia zgody, jeżeli przetwarzanie odbywa się na podstawie zgody, oraz wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
 9. Podanie danych oznaczonych jako niezbędne jest warunkiem udziału w Projekcie. Niepodanie tych danych może uniemożliwić udział w rekrutacji albo w danej formie

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

wsparcia. Wyrażenie zgody na wykorzystanie wizerunku w celach promocyjnych jest dobrowolne i nie wpływa na możliwość udziału w Projekcie. Brak akceptacji nagrywanego trybu realizacji Szkolenia uniemożliwia udział w tej edycji Szkolenia. Nie dotyczy to dobrowolnej zgody na publiczne wykorzystanie wizerunku lub głosu w celach promocyjnych.

§ 16. Wizerunek, dokumentacja fotograficzna i nagrania

1. Szkolenie realizowane jest w formule nagrywanej. Nagranie obejmuje obraz i dźwięk przebiegu zajęć, w tym wypowiedzi prowadzących, prezentacje, pytania, dyskusje oraz wypowiedzi Uczestników.
2. Udział w nagrywanym Szkoleniu wymaga uprzedniego przyjęcia przez Uczestnika do wiadomości zasad nagrywania określonych w Regulaminie oraz potwierdzenia akceptacji nagrywanego trybu realizacji Szkolenia.
3. Nagrania są udostępniane wyłącznie w zamkniętym środowisku technicznym, w zakresie niezbędnym do realizacji Szkolenia, Uczestnikom danej edycji, prowadzącym, upoważnionym członkom zespołu projektowego, administratorom technicznym Platformy oraz podmiotom uprawnionym do kontroli lub audytu Projektu.
4. Nagrania nie są publikowane publicznie, w szczególności na stronie internetowej Projektu, stronie internetowej Politechniki Śląskiej, w mediach społecznościowych ani w materiałach promocyjnych, na podstawie samej akceptacji nagrywanego trybu realizacji Szkolenia.
5. Publiczne wykorzystanie lub rozpowszechnianie wizerunku albo głosu Uczestnika w materiałach informacyjnych, promocyjnych, medialnych albo upowszechniających rezultaty Projektu wymaga odrębnej, dobrowolnej zgody, chyba że przepisy prawa stanowią inaczej.
6. Brak zgody na publiczne wykorzystanie wizerunku albo głosu nie wpływa na możliwość udziału w Szkoleniu ani otrzymania dokumentu potwierdzającego jego ukończenie.
7. Uczestnik nie może samodzielnie nagrywać zajęć, kopiować nagrań, fotografować materiałów egzaminacyjnych ani rozpowszechniać wizerunku, głosu lub wypowiedzi prowadzących albo innych Uczestników bez wymaganych uprawnień i zgód.

§ 17. Materiały szkoleniowe, prawa autorskie i poufność

1. Materiały szkoleniowe, nagrania, testy, zadania, prezentacje, publikacje, wzory dokumentów i inne treści udostępniane w ramach Projektu podlegają ochronie prawnej.

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

2. Uczestnik może korzystać z materiałów szkoleniowych wyłącznie w celu udziału w Projekcie, samokształcenia oraz – jeżeli Organizator tak postanowi – wewnętrznego wykorzystania w instytucji delegującej w zakresie zgodnym z przeznaczeniem materiałów.
3. Zakazane jest kopiowanie, rozpowszechnianie, publikowanie w Internecie, odsprzedaż, udzielanie sublicencji, usuwanie oznaczeń, modyfikowanie materiałów albo wykorzystywanie ich komercyjnie bez zgody Organizatora lub uprawnionego podmiotu.
4. Uczestnik zobowiązuje się zachować w poufności informacje uzyskane w toku zajęć, jeżeli dotyczą one bezpieczeństwa, infrastruktury, procedur, dokumentacji, incydentów, podatności, konfiguracji, tajemnic przedsiębiorstwa, tajemnic prawnie chronionych albo informacji oznaczonych jako poufne.
5. Prawa autorskie do utworów powstałych w ramach Projektu są regulowane umową zawartą pomiędzy Politechniką Śląską a Ministrem Nauki i Szkolnictwa Wyższego oraz właściwymi umowami z twórcami, prowadzącymi, wykonawcami i podmiotami trzecimi.
6. Materiały szkoleniowe oraz inne utwory powstałe w ramach Projektu mogą być wykorzystywane przez Organizatora oraz Ministra Nauki i Szkolnictwa Wyższego w zakresie wynikającym z umowy o finansowanie Projektu oraz obowiązujących przepisów prawa.

§ 18. Informacje o Projekcie i publikacja danych Uczestników

1. Informacje o Projekcie, rekrutacji, harmonogramach i formach wsparcia są publikowane na stronie internetowej Projektu: **cyberedu.polsl.pl** oraz mogą być przekazywane Kandydatom i Uczestnikom za pośrednictwem poczty elektronicznej albo Platformy.
2. Organizator nie publikuje imiennych list Kandydatów, Uczestników, osób zakwalifikowanych, osób wpisanych na listę rezerwową ani wyników testów lub egzaminów, chyba że istnieje wyraźna podstawa prawna publikacji, osoba, której dane dotyczą, udzieliła właściwej zgody albo dane zostały skutecznie zanonimizowane.
3. Publikacja wizerunku Uczestnika w materiałach informacyjnych lub promocyjnych Projektu wymaga odrębnej podstawy prawnej, w szczególności dobrowolnej zgody, chyba że przepisy prawa dopuszczają rozpowszechnianie wizerunku bez zgody.

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

§ 19. Skargi, reklamacje i uwagi

1. Uczestnik może zgłosić do Biura Projektu, Kierownika Projektu albo zespołu projektowego uwagę albo skargę dotyczącą organizacji, dostępności, jakości zajęć, działania Platformy, naruszenia Regulaminu albo procesu rekrutacji.
2. Zgłoszenie powinno zawierać imię i nazwisko, dane kontaktowe, nazwę formy wsparcia, opis sprawy oraz oczekiwany sposób rozpatrzenia.
3. Organizator rozpatruje zgłoszenie bez zbędnej zwłoki, co do zasady w terminie 14 dni roboczych od dnia jego otrzymania. W sprawach wymagających dodatkowych wyjaśnień termin może zostać przedłużony, o czym osoba zgłaszająca zostanie poinformowana.
4. Zgłoszenia dotyczące ochrony danych osobowych mogą być kierowane bezpośrednio do Inspektora Ochrony Danych.

§ 20. Zmiany Regulaminu

1. Organizator może zmienić Regulamin w przypadku zmiany umowy z Ministrem, harmonogramu Projektu, przepisów prawa, wytycznych, dokumentów wewnętrznych Politechniki Śląskiej, zasad finansowania, wymagań organizacyjnych albo innych okoliczności wpływających na prawidłową realizację Projektu.
2. Zmiany Regulaminu obowiązują od dnia wskazanego przez Organizatora, nie wcześniej jednak niż od dnia ich opublikowania na stronie internetowej Projektu: **cyberedu.polsl.pl** albo przekazania Uczestnikom za pośrednictwem poczty elektronicznej lub Platformy, chyba że zmiana wynika bezpośrednio z przepisów prawa albo umowy z Ministrem.
3. Zmiany Regulaminu nie mogą naruszać praw nabytych Uczestników w sposób nieproporcjonalny, chyba że jest to konieczne z uwagi na przepisy prawa, bezpieczeństwo, dostępność, ochronę danych, decyzję Ministra, organów kontroli albo prawidłowe rozliczenie Projektu.

§ 21. Postanowienia końcowe

1. Regulamin wchodzi w życie z dniem jego zatwierdzenia w trybie obowiązującym w Politechnice Śląskiej.
2. Regulamin obowiązuje przez okres realizacji Projektu oraz, w zakresie dotyczącym dokumentowania udziału, archiwizacji dokumentów uczestnictwa, praw autorskich,

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253

poufności, ochrony danych osobowych i rozpatrywania spraw związanych z udziałem Uczestnika, także po zakończeniu udziału Uczestnika w Projekcie.

3. W sprawach nieuregulowanych Regulaminem stosuje się przepisy prawa powszechnie obowiązującego, umowę zawartą z Ministrem, dokumenty projektowe oraz akty wewnętrzne Politechniki Śląskiej.
4. Aktualna wersja Regulaminu jest dostępna na stronie internetowej Projektu: cyberedu.polsl.pl oraz w Biurze Projektu pod adresem: Politechnika Śląska, Wydział Automatyki, Elektroniki i Informatyki, ul. Akademicka 16, pok. 408, 44-100 Gliwice, e-mail: Dorota.Huget@polsl.pl, tel. +48 32 237 13 39.
5. Załączniki do Regulaminu stanowią jego integralną część, o ile zostały wyraźnie oznaczone jako załączniki.

Wykaz załączników stanowiących integralną część Regulaminu

1. Załącznik nr 1 – Formularz zgłoszeniowy Kandydata.
2. Załącznik nr 2 – Deklaracja uczestnictwa i akceptacja Regulaminu.
3. Załącznik nr 3 – Potwierdzenie delegowania przez instytucję.
4. Załącznik nr 4 – Klauzula informacyjna RODO dla Kandydatów i Uczestników.
5. Załącznik nr 5 – Oświadczenie o potrzebach dostępności / wniosek o zapewnienie dostępności.
6. Załącznik nr 6 – Dobrowolna zgoda na wykorzystanie wizerunku.
7. Załącznik nr 7 – Oświadczenie o rezygnacji z udziału w Projekcie.

Projekt finansowany ze środków Ministra Nauki i Szkolnictwa Wyższego w ramach zadania badawczego pn.: „Podnoszenie kompetencji z zakresu cyberbezpieczeństwa poprzez realizację szkoleń dla podmiotów systemu szkolnictwa wyższego i nauki”.

Dofinansowanie: 2 999 400 zł | Całkowita wartość: 2 999 400 zł | UMOWA Nr MNiSW/2026/DIR/253