

## ZAŁĄCZNIK NR 1B DO SWZ

## OPIS PRZEDMIOTU ZAMÓWIENIA - PAKIET 1

## ZAKRES ZAMÓWIENIA

Przedmiotem zamówienia jest aktualizacja SZBI poprzez wdrożenie 9 polityk bezpieczeństwa oraz udostępnienie platformy szkoleniowej ze szkoleniami o tematyce podnoszącej poziom cyberbezpieczeństwa dla kadry kierowniczej, medycznej i administracyjnej, w tym w szczególności wykonanie następujących zadań:

Zakres zamówienia objęty jest Wniosem o wsparcie w zakresie:

Zadanie 3: Działania zwiększające poziom cyberbezpieczeństwa szpitala

- I. Aktualizacja SZBI - wdrożenie 9 polityk - koszt 3.17
- II. Szkolenie kadry kierowniczej - koszt. 3.18
- III. Szkolenie kadry medycznej - koszt 3.19
- IV. Szkolenia kadry administracyjnej - koszt 3.20

## A. TERMIN REALIZACJI

Wykonawca zobowiązany jest do wykonania przedmiotu umowy nie później niż do dnia 20 czerwca 2026 roku.

## B. GWARANCJA JAKOŚCI

W ramach zamówienia wykonawca udzieli na wykonane usługi gwarancji jakości na okres nie krótszy niż 12 miesięcy od daty podpisania protokołu odbioru prawidłowo wykonanego przedmiotu zamówienia.

## C. OPIS MINIMALNYCH WYMAGAŃ FUNKCJONALNYCH I TECHNICZNYCH

## I. Aktualizacja SZBI - wdrożenie 9 polityk

Przedmiotem zamówienia jest wykonanie aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji posiadanej przez Zamawiającego.

## I.1 Aktualizacji 9 polityk bezpieczeństwa:

Lp.	Polityka
1	zarządzania dostępem i uprawnieniami
2	kryptografii z uwzględnieniem zalecanych dopuszczalnych protokołów szyfrowania
3	zarządzania podatnościami
4	zarządzania ryzykiem z uwzględnieniem obszaru cyberbezpieczeństwa
5	logowania zdarzeń z uwzględnieniem aplikacji, sieci, serwerów, bramy brzegowej, kontrolerem domeny
6	kopii bezpieczeństwa
7	zarządzania incydentami bezpieczeństwa
8	zarządzania ciągłością działania
9	ochrony danych osobowych z uwzględnieniem przetwarzania danych medycznych

## I.2 Wdrożenie oprogramowania do utrzymania SZBI w aktualności

Lp.	Wymaganie	Wymagane parametry funkcjonalne
1	Zakres	1. Do obowiązków Wykonawcy w ramach niniejszego zadania należy wdrożenie oprogramowania do utrzymania w aktualności Systemu Zarządzania Bezpieczeństwem Informacji
2	Użytkownicy	1. Synchronizacja użytkowników systemu z Active Directory. 2. Możliwość nadawania użytkownikom różnych uprawnień.
3	Słowniki	3. Jednostki odzwierciedlające hierarchiczną strukturę organizacyjną. 4. Cele kontroli w ramach doskonalenia SZBI. 5. Dokumenty stanowiące SZBI (lista polityk, procedur, zasad i innych dokumentów, które będą poddawane cyklicznej kontroli pod kątem aktualności i adekwatności). 6. Mechanizmy kontrolne (lista stosowanych zabezpieczeń technicznych i organizacyjnych wraz z możliwością określenia ich rodzaju i roli w SZBI). 7. Usługi kluczowe
4	Checklisty	8. Predefiniowane checklisty pozwalające na przeprowadzenie audytu SZBI. 9. Tworzenie własnych wielopoziomowych checklist służących do przeprowadzania kontroli i udzielania jednoznacznych odpowiedzi na każde pytanie.
5	Plany kontroli	10. Tworzenie długoterminowych planów kontroli. 11. Proces akceptacji poszczególnych planów kontroli (możliwość akceptacji planów przez osobę tworzącą).
6	Programy testowania	1. Tworzenie programów testowania w podziale na obszary objęte kontrolą, okresy, systemy i osoby. 2. Proces akceptacji poszczególnych programów. 3. Definiowanie próby kontrolnej - możliwość zdefiniowania próby kontrolnej do badania
7	Badanie	1. Przeprowadzanie badania na bazie checklisty - możliwość przeprowadzenia badania na bazie checklisty dla każdego przypadku testowego w ramach próby. Zabezpieczenie przed pominięciem odpowiedzi na pytania z checklisty podczas badania. 2. Możliwość weryfikacji wyników badania przez kontrolowanego pracownika. 3. Zamykanie badania przez kontrolera - kończenie badania i akceptacja wyników kontroli celem generowania nieprawidłowości i zaleceń
8	Nieprawidłowości	1. Rejestr nieprawidłowości – ewidencja nieprawidłowości wykrytych podczas audytów SZBI. 2. Automatyczne generowanie nieprawidłowości z badania na podstawie udzielonych odpowiedzi - generowanie nieprawidłowości w oparciu o szablon treści nieprawidłowości powiązany z pytaniami na checkliście. 3. Możliwość ręcznego dodawania nieprawidłowości wykrytych podczas kontroli. 4. Proces zarządzania nieprawidłowościami (ewidencja, zatwierdzanie, zamykanie).
9	Zalecenia	1. Rejestr zaleceń – prowadzenie ewidencji zaleceń wydanych podczas audytów SZBI. 2. Automatyczne generowanie zaleceń po badaniu na podstawie udzielonych odpowiedzi - generowanie zaleceń w oparciu o szablon treści zaleceń powiązany z pytaniami na checkliście. 3. Możliwość ręcznego dodawania zaleceń. 4. Proces akceptacji poszczególnych zaleceń w zakresie zatwierdzenia ich realizacji (terminy, osoby odpowiedzialne, koszty). 5. Proces zatwierdzania poszczególnych zaleceń pod kątem sposobu ich realizacji (weryfikacja czy zalecenie zrealizowane zgodnie z wytycznymi). 6. Możliwość importu zaleceń z pliku. 7. Przypisywanie zaleceń do projektów.
10	Rejestry SZBI	1. Rejestr aktywów – prowadzenie ewidencji aktywów wraz z możliwością ewidencji danych dotyczących wsparcia serwisowego dla danego aktywa i zagrożeń związanych z jego brakiem. 2. Rejestr systemów – prowadzenie ewidencji systemów informatycznych wraz z możliwością klasyfikacji tych systemów według atrybutów poufności, integralności i dostępności. 3. Rejestr procesów - prowadzenie ewidencji procesów wraz z ewidencją danych dotyczących wpływu zakłóceń na proces, RTO, RPO, MTD oraz pozwalających na przeprowadzanie analizy BIA dla procesu. 4. Rejestr obszarów bezpiecznych – prowadzenie ewidencji obszarów bezpiecznych wraz z możliwością wskazywania stosowanych zabezpieczeń organizacyjnych i technicznych w danym obszarze. 5. Rejestr nośników – prowadzenie ewidencji nośników danych wraz z możliwością ewidencji informacji wynikających z procedury bezpiecznego usuwania nośników.

		<ol style="list-style-type: none"> <li>Rejestr kopii zapasowych – prowadzenie ewidencji kopii zapasowych wraz z możliwością ewidencji szczegółowych informacji o jej wykonywaniu, składowaniu i weryfikacji poprawności jej odtwarzania.</li> <li>Rejestr informacji – prowadzenie ewidencji informacji wraz z możliwością klasyfikacji tych informacji według atrybutów poufności, integralności i dostępności.</li> <li>Rejestr incydentów - prowadzenie ewidencji wykrytych incydentów wraz z jego oceną i klasyfikacją, określeniem rodzaju i skali incyduentu oraz jego potencjalnego wpływu na jednostkę wraz z kontrolą poprawności i terminowości obowiązku informacyjnego dotyczącego zgłaszania incydentów.</li> <li>Rejestr ryzyk - identyfikacja ryzyk wraz z możliwością szacowania i oceny, kontroli i monitorowania ryzyka.</li> <li>Rejestr czynności przetwarzania danych osobowych - prowadzenie rejestru czynności przetwarzania realizowanych zarówno jako administrator danych, które w danej czynności są przetwarzane jak i jako podmiot przetwarzający dane osobowe (RODO).</li> <li>Rejestr upoważnień - ewidencja nadanych uprawnień do systemów - prowadzenie ewidencji upoważnień do systemów informatycznych, do których użytkownik ma mieć dostęp, szkoleń dotyczących ochrony danych i podpisanych upoważnień do przetwarzania danych osobowych.</li> <li>Rejestr zmian – prowadzenie ewidencji planowanych i realizowanych zmian w systemach informatycznych wraz z możliwością śledzenia poszczególnych etapów wdrożeń oraz analizy pod kątem planowanych i rzeczywistych terminów i kosztów realizacji.</li> <li>Rejestr kluczowych dostawców – prowadzenie ewidencji kluczowych dostawców usług i sprzętu wraz z analizą ryzyka związanego z upadłością dostawcy i oceny zdolności dostawcy do zachowania ciągłości działa i jakości poziomu świadczonych usług</li> </ol>
11	Raporty	<ol style="list-style-type: none"> <li>Raport z planów kontroli - format xls lub pdf z możliwością parametryzacji raportu</li> <li>Raport z programów badań - format xls lub pdf z możliwością parametryzacji raportu</li> <li>Raport z realizacji zaleceń - format xls lub pdf z możliwością parametryzacji raportu</li> <li>Raport z nieprawidłowości - format xls lub pdf z możliwością parametryzacji raportu</li> <li>Raport z rejestru systemów - format xls lub pdf z możliwością parametryzacji raportu</li> <li>Raport z rejestru aktywów - format xls lub pdf z możliwością parametryzacji raportu</li> <li>Raport z rejestru systemów - format xls lub pdf z możliwością parametryzacji raportu</li> <li>Raport z rejestru procesów - format xls lub pdf z możliwością parametryzacji raportu</li> <li>Raport z rejestru nośników - format xls lub pdf z możliwością parametryzacji raportu</li> <li>Raport z rejestru kopii zapasowych - format xls lub pdf z możliwością parametryzacji raportu</li> <li>Raport z rejestru obszarów bezpiecznych - format xls lub pdf z możliwością parametryzacji raportu</li> <li>Raport z rejestru informacji - format xls lub pdf z możliwością parametryzacji raportu</li> <li>Raport z rejestru zmian - format xls lub pdf z możliwością parametryzacji raportu</li> <li>Raport z rejestru ryzyk- format xls lub pdf z możliwością parametryzacji raportu</li> <li>Raport z rejestru czynności przetwarzania- format xls lub pdf z możliwością parametryzacji raportu</li> <li>Raport z rejestru incydentów- format xls lub pdf z możliwością parametryzacji raportu</li> <li>Raport z rejestru upoważnień- format xls lub pdf z możliwością parametryzacji raportu</li> <li>Sprawozdanie z audytu – model porównawczy w stosunku do poprzedniego audytu oraz poprzedniego do poprzedniego</li> <li>Protokół pokontrolny - format doc lub pdf automatycznie generowany na podstawie danych z przeprowadzonego badania.</li> </ol>
12	Model wdrożenia	<ol style="list-style-type: none"> <li>Oprogramowania do audytu i utrzymania SZBI powinno zostać wdrożone w modelu subskrypcyjnym SaaS (Software as a Service) na zasobach spełniających następujące wymagania bezpieczeństwa: <ol style="list-style-type: none"> <li>Certyfikat ISO 27001 - wymagania dotyczące systemu zarządzania bezpieczeństwem informacji</li> <li>Certyfikat ISO 27018 - bezpieczeństwo przetwarzania i ochrony danych osobowych w chmurze</li> </ol> </li> <li>Oprogramowania wdrożone w modelu SaaS z prawem dostępu dla minimum 10 użytkowników Zamawiającego.</li> <li>Minimalny okres trwania licencji/ subskrypcji – 36 miesięcy.</li> <li>Cena wdrożenia i zaoferowanego czasu licencji/ subskrypcji powinna być zawarta w cenie oferty.</li> <li>Zaoferowane rozwiązanie powinno charakteryzować się skalowalnością i odpornością na awarię.</li> <li>Minimalny poziom dostępności aplikacji – 99%.</li> <li>Konieczne aktualizacje oprogramowania powinny dokonywać się automatycznie bez udziału Zamawiającego.</li> </ol>
13	Instruktaż	Instruktaż max 5 osób wskazanych przez Zamawiającego z obsługi wdrożonego rozwiązania

## II. Szkolenie kadry kierowniczej

Lp.	Wymaganie	Wymagane parametry funkcjonalne
1	Cel	Podniesienie świadomości kadry kierowniczej w zakresie Cyberbezpieczeństwa
2	Zakres szkolenia	<ol style="list-style-type: none"> <li>1. Podstawy prawne w obszarze cyberbezpieczeństwa (KRI, KSC i RODO, NIS2)</li> <li>2. Proces utrzymania SZBI w aktualności</li> <li>3. Typy ataków wraz z przykładami (phishing, ransomware, fałszywe logowania),</li> <li>4. Reagowanie na incydenty</li> <li>5. Waga wykonywania badań bezpieczeństwa</li> <li>6. Rola kadry zarządzającej w procesach bezpieczeństwa</li> </ol>
3	Uczestnicy	Kadra kierownicza – maksymalnie 50 osób
4	Forma	<ol style="list-style-type: none"> <li>1. Platforma szkoleniowa (portal internetowy):               <ol style="list-style-type: none"> <li>a) Dostęp online 24/7 przez cały okres trwania umowy.</li> <li>b) Zamieszczenie wszystkich materiałów szkoleniowych (np. filmy, prezentacje, dokumenty PDF).</li> <li>c) Rejestracja uczestnictwa</li> <li>d) Dostęp do portalu dla minimum 50 użytkowników jednocześnie</li> </ol> </li> <li>2. Zamawiający wymaga, aby platforma szkoleniowa posiadała mechanizm uwierzytelniania użytkowników umożliwiający logowanie:               <ol style="list-style-type: none"> <li>a) za pomocą indywidualnego loginu oraz hasła,</li> <li>b) alternatywnie za pomocą adresu poczty elektronicznej.</li> </ol>               Oba sposoby logowania muszą funkcjonować równolegle i zapewniać pełny, równoważny dostęp do wszystkich funkcjonalności platformy, zgodnie z nadanymi uprawnieniami użytkownika.                Mechanizm logowania powinien spełniać aktualne standardy bezpieczeństwa, w szczególności:               <ol style="list-style-type: none"> <li>a) zapewniać poufność danych uwierzytelniających,</li> <li>b) umożliwiać stosowanie silnych haseł,</li> <li>c) zabezpieczać proces logowania przed nieautoryzowanym dostępem.</li> </ol> </li> </ol>
5	Materiały szkoleniowe	<ol style="list-style-type: none"> <li>1. Materiały powinny być dostępne do pobrania lub wydrukowania dla uczestników.</li> <li>2. Treści aktualizowane przynajmniej raz do roku zgodnie z aktualnymi standardami i przepisami</li> </ol>
6	Monitoring	<ol style="list-style-type: none"> <li>1. Możliwość bieżącego monitorowania iloczby osób, które przystąpiły do szkolenia</li> <li>2. Raportowanie powinno obejmować liczbę uczestników</li> <li>3. Potwierdzenie ukończenia szkolenia:               <ol style="list-style-type: none"> <li>a) uczestnik po ukończeniu szkolenia powinien być oznaczony jako osoba, która zrealizowała obowiązek szkoleniowy.</li> <li>b) Certyfikat potwierdzający ukończenie szkolenia</li> </ol> </li> </ol>
7	Wsparcie techniczne i organizacyjne	<ol style="list-style-type: none"> <li>1. Dostęp do wsparcia technicznego dla użytkowników platformy.</li> <li>2. Dostępność pomocy organizacyjnej w godzinach roboczych (telefonicznej i mailowej).</li> <li>3. Bezpieczeństwo i ochrona danych: Wszystkie dane użytkowników muszą być zabezpieczone</li> </ol>
8	Okres trwania	<ol style="list-style-type: none"> <li>1. Szkolenia mają zostać przeprowadzone do 20 czerwca 2026 roku</li> <li>2. Wymagana dostępność platformy wraz z materiałami szkoleniowymi do 20 czerwca 2029 roku.</li> </ol>

### III. Szkolenie kadry medycznej

Lp.	Wymaganie	Wymagane parametry funkcjonalne
1	Cel	Podniesienie świadomości kadry medycznej w zakresie Cyberbezpieczeństwa
2	Zakres szkolenia	<ol style="list-style-type: none"> <li>1. Podstawowe zasady cyberhigieny</li> <li>2. Bezpieczeństwo haseł i uwierzytelniania (MFA, menedżery haseł, ryzyka stosowania słabych haseł).</li> <li>3. Bezpieczne korzystanie z poczty (rozpoznawanie podejrzanych wiadomości, załączników, linków).</li> <li>4. Zasady pracy na stanowisku (blokowanie ekranu, czyste biurko, brak udostępniania kontTypy ataków wraz z przykładami (phishing, ransomware, fałszywe logowania),</li> <li>5. Reagowanie na incydenty</li> <li>6. Ciągłość działania</li> <li>7. Zarządzanie ryzykiem w bezpieczeństwie informacji i obszarach technicznych.</li> <li>8. Zasady zarządzania bezpieczeństwem informacji – SZBI.</li> <li>9. Postępowanie w przypadku incyduentu (kogo powiadomić, jak nie pogorszyć sytuacji, rola CSIRT CeZ)</li> <li>10. Bezpieczna obsługa systemów medycznych (EDM, eZLA, HIS, PACS/RIS) zgodnie z praktyką CeZ i ZUS.</li> <li>11. Ochrona danych pacjentów i RODO (co wolno, czego nie wolno, minimalizacja danych, zgłaszanie naruszeń).</li> </ol>
3	Uczestnicy	Kadra medyczna – maksymalnie 1000 osób
4	Forma	<ol style="list-style-type: none"> <li>1. Platforma szkoleniowa (portal internetowy):               <ol style="list-style-type: none"> <li>a) Dostęp online 24/7 przez cały okres trwania umowy.</li> <li>b) Zamieszczenie wszystkich materiałów szkoleniowych (np. filmy, prezentacje, dokumenty PDF).</li> <li>c) Rejestracja uczestnictwa</li> <li>d) Dostęp do portalu dla minimum 50 użytkowników jednoczesnych</li> </ol> </li> <li>2. Zamawiający wymaga, aby platforma szkoleniowa posiadała mechanizm uwierzytelniania użytkowników umożliwiający logowanie:               <ol style="list-style-type: none"> <li>a) za pomocą indywidualnego loginu oraz hasła,</li> <li>b) alternatywnie za pomocą adresu poczty elektronicznej.</li> </ol>               Oba sposoby logowania muszą funkcjonować równolegle i zapewniać pełny, równoważny dostęp do wszystkich funkcjonalności platformy, zgodnie z nadanymi uprawnieniami użytkownika.                Mechanizm logowania powinien spełniać aktualne standardy bezpieczeństwa, w szczególności:               <ol style="list-style-type: none"> <li>a) zapewniać poufność danych uwierzytelniających,</li> <li>b) umożliwiać stosowanie silnych haseł,</li> <li>c) zabezpieczać proces logowania przed nieautoryzowanym dostępem.</li> </ol> </li> <li>3. Zamawiający wymaga, aby platforma szkoleniowa posiadała mechanizm sprawdzenia użytkownika ze zrozumienia materiału (z podaniem wyniku procentowego).</li> </ol>
5	Materiały szkoleniowe	<ol style="list-style-type: none"> <li>1. Materiały powinny być dostępne do pobrania lub wydrukowania dla uczestników.</li> <li>2. Treści aktualizowane przynajmniej raz do roku zgodnie z aktualnymi standardami i przepisami</li> </ol>
6	Monitoring	<ol style="list-style-type: none"> <li>1. Możliwość bieżącego monitorowania iloczby osób, które przystąpiły do szkolenia</li> <li>2. Raportowanie powinno obejmować liczbę uczestników</li> <li>3. Potwierdzenie ukończenia szkolenia:               <ol style="list-style-type: none"> <li>a) uczestnik po ukończeniu szkolenia powinien być oznaczony jako osoba, która zrealizowała obowiązek szkoleniowy.</li> <li>b) Certyfikat potwierdzający ukończenie szkolenia</li> </ol> </li> </ol>
7	Wsparcie techniczne i organizacyjne	<ol style="list-style-type: none"> <li>1. Dostęp do wsparcia technicznego dla użytkowników platformy.</li> <li>2. Dostępność pomocy organizacyjnej w godzinach roboczych (telefonicznej i mailowej).</li> <li>3. Bezpieczeństwo i ochrona danych: Wszystkie dane użytkowników muszą być zabezpieczone</li> </ol>
8	Okres trwania	<ol style="list-style-type: none"> <li>1. Szkolenia mają zostać przeprowadzone do 20 czerwca 2026 roku</li> <li>2. Wymagana dostępność platformy wraz z materiałami szkoleniowymi do 20 czerwca 2029 roku.</li> </ol>

#### IV. Szkolenia kadry administracyjnej

Lp.	Wymaganie	Wymagane parametry funkcjonalne
1	Cel	Podniesienie świadomości kadry administracyjnej w zakresie Cyberbezpieczeństwa
2	Zakres szkolenia	<ol style="list-style-type: none"> <li>1. Podstawowe zasady cyberhigieny</li> <li>2. Bezpieczeństwo haseł i uwierzytelniania (MFA, menedżery haseł, ryzyka stosowania słabych haseł).</li> <li>3. Bezpieczne korzystanie z poczty (rozpoznawanie podejrzanych wiadomości, załączników, linków).</li> <li>4. Zasady pracy na stanowisku (blokowanie ekranu, czyste biurko, brak udostępniania kontTypy ataków wraz z przykładami (phishing, ransomware, fałszywe logowania),</li> <li>5. Reagowanie na incydenty</li> <li>6. Ciągłość działania</li> <li>7. Zarządzanie ryzykiem w bezpieczeństwie informacji i obszarach technicznych.</li> <li>8. Zasady zarządzania bezpieczeństwem informacji – SZBI.</li> <li>9. Postępowanie w przypadku incydentu (kogo powiadomić, jak nie pogorszyć sytuacji, rola CSIRT CeZ)</li> <li>10. Bezpieczna obsługa systemów medycznych (EDM, eZLA, HIS, PACS/RIS) zgodnie z praktyką CeZ i ZUS.</li> <li>11. Ochrona danych pacjentów i RODO (co wolno, czego nie wolno, minimalizacja danych, zgłaszanie naruszeń).</li> </ol>
3	Uczestnicy	Kadra administracyjna – maksymalnie 100 osób
4	Forma	<ol style="list-style-type: none"> <li>1. Platforma szkoleniowa (portal internetowy): <ol style="list-style-type: none"> <li>a) Dostęp online 24/7 przez cały okres trwania umowy.</li> <li>b) Zamieszczenie wszystkich materiałów szkoleniowych (np. filmy, prezentacje, dokumenty PDF).</li> <li>c) Rejestracja uczestnictwa</li> <li>d) Dostęp do portalu dla minimum 50 użytkowników jednoczesnych</li> </ol> </li> <li>2. Zamawiający wymaga, aby platforma szkoleniowa posiadała mechanizm uwierzytelniania użytkowników umożliwiający logowanie: <ol style="list-style-type: none"> <li>a) za pomocą indywidualnego loginu oraz hasła,</li> <li>b) alternatywnie za pomocą adresu poczty elektronicznej.</li> </ol> Oba sposoby logowania muszą funkcjonować równolegle i zapewniać pełny, równoważny dostęp do wszystkich funkcjonalności platformy, zgodnie z nadanymi uprawnieniami użytkownika.  Mechanizm logowania powinien spełniać aktualne standardy bezpieczeństwa, w szczególności: <ol style="list-style-type: none"> <li>a) zapewniać poufność danych uwierzytelniających,</li> <li>b) umożliwiać stosowanie silnych haseł,</li> <li>c) zabezpieczać proces logowania przed nieautoryzowanym dostępem.</li> </ol> </li> </ol>
5	Materiały szkoleniowe	<ol style="list-style-type: none"> <li>1. Materiały powinny być dostępne do pobrania lub wydrukowania dla uczestników.</li> <li>2. Treści aktualizowane przynajmniej raz do roku zgodnie z aktualnymi standardami i przepisami</li> </ol>
6	Monitoring	<ol style="list-style-type: none"> <li>1. Możliwość bieżącego monitorowania iloczby osób, które przystąpiły do szkolenia</li> <li>2. Raportowanie powinno obejmować liczbę uczestników</li> <li>3. Potwierdzenie ukończenia szkolenia: <ol style="list-style-type: none"> <li>a) uczestnik po ukończeniu szkolenia powinien być oznaczony jako osoba, która zrealizowała obowiązek szkoleniowy.</li> <li>b) Certyfikat potwierdzający ukończenie szkolenia</li> </ol> </li> </ol>
7	Wsparcie techniczne i organizacyjne	<ol style="list-style-type: none"> <li>1. Dostęp do wsparcia technicznego dla użytkowników platformy.</li> <li>2. Dostępność pomocy organizacyjnej w godzinach roboczych (telefonicznej i mailowej).</li> <li>3. Bezpieczeństwo i ochrona danych: Wszystkie dane użytkowników muszą być zabezpieczone</li> </ol>
8	Okres trwania	<ol style="list-style-type: none"> <li>1. Szkolenia mają zostać przeprowadzone do 20 czerwca 2026 roku</li> <li>2. Wymagana dostępność platformy wraz z materiałami szkoleniowymi do 20 czerwca 2029 roku.</li> </ol>