Załącznik nr 1

Opis przedmiotu zamówienia

Wykonawca zobowiązuje się do realizacji przedmiotu zamówienia zgodnie z poniższym zakresem:

1. Dostawa serwera do wykonywania kopii zapasowych

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania minimum dwóch procesorów. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	• Zainstalowany jeden procesor 12-rdzeniowy klasy x86, min. 2.1GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 174 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	• 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.
Funkcjonalność pamięci RAM	• Advanced ECC, • Memory Page Retire, • Fault Resilient Memory, • Memory Self-Healing lub PPR, • Partial Cache Line Sparing
Gniazda PCI	• minimum 2 sloty PCIe z czego przynajmniej trzy generacji 4
Interfejsy sieciowe/SAS	• Wbudowane min. 6 interfejsów sieciowych 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) • Dodatkowa, czteroportowa karta 12Gb SAS HBA
Dyski twarde	• Zainstalowane: o 8x dysk SSD SATA o pojemności min. 960GB, 2,5“ Hot-Plug.

	• Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. • Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający o Min. 8GB nieulotnej pamięci cache, o Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. o Wsparcie dla dysków samoszyfrujących.
Wbudowane porty	• Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, • Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	• Redundantne, Hot-Plug min. 1100W klasy Titanium
System operacyjny/dodatkowe oprogramowanie	• Windows Server 2022 Standard
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	• Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: o zdalny dostęp do graficznego interfejsu Web karty zarządzającej; o zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); o szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; o możliwość podmontowania zdalnych wirtualnych napędów;

	○ wirtualną konsolę z dostępem do myszy, klawiatury; ○ wsparcie dla IPv6; ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ○ integracja z Active Directory; ○ możliwość obsługi przez dwóch administratorów jednocześnie; ○ wsparcie dla dynamic DNS; ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia

	○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is" do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych

	plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku – **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Gwarancji producenta: …….(wartość 36 lub 60 m/cy zostanie uzupełniona na podstawie oferty Wykonawcy). • Możliwość rozszerzenia gwarancji przez producenta do 7 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.

	• Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. • Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

2. Dostawa oprogramowania do wykonywania kopii zapasowych – 2 sztuki

Oprogramowania do zabezpieczania danych poprzez mechanizm kopi zapasowych dedykowane dla środowisk serwerowych.

1. Oprogramowanie musi wspierać co najmniej systemy operacyjne:
   - Windows XP i nowsze.
   - Windows Server 2003 i nowsze.
   - Windows SBS 2011/2008, 2003/2003R2.
   - Windows Storage Server 2012/2012R2, 2008R2/2008/2003.
   - Windows MultiPoint Server 2012/2011/2010.
   - Linux.

2. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:
   - Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www.
   - Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego).
   - Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych.

- Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu).
- Możliwość definiowania uprawnień dla administratorów system kopi zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.).
- Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami.
- Wsparcie dla Single Sign On dla logowania do systemu.
- Możliwość zarządzania procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT.
- Możliwość definiowania planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem).
- Możliwość tworzenia zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopi zapasowych.
- Możliwość zdalnej instalacji agentów kopi zapasowych na maszynach z systemem operacyjnym Windows.
- Możliwość zdalnego uaktualniania agentów kopi zapasowych.
- Możliwość zdalnego zarządzania procesem wykonywania kopii zapasowej i odzyskiwania danych.
- Możliwość zdefiniowania dedykowanej maszyny, której agent kopi zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej).
- Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych.
- Centralny katalog wszystkich danych zapisanych w kopiach zapasowych.
- Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.

3. Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:
   - Kopie zapasowe całych dysków i partycji.
   - Kopie zapasowe wybranych plików i folderów.
   - Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory)
   - Kopie zapasowe baz danych Oracle.
   - Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych.
   - Zapis kopi zapasowych na udziały sieciowe.
   - Zapis kopi zapasowych na serwer SFTP.
   - Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana.
   - Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery).
   - Możliwość wyszukiwania plików w kopiach zapasowych.
   - Możliwość szyfrowania plików kopi zapasowych.
   - Wsparcia dla technologii VSS.

- Deduplikacja kopi zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć.
- Kompresja plików kopi zapasowych.
- Możliwość replikacji kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy).
- Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.

4. Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:
   - Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore.
   - Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową.
   - Odtworzenie poszczególnych plików i folderów.
   - Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowania maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania).
   - Granularne odtwarzanie baz danych Microsoft Exchange.
   - Granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange.
   - Wyszukiwanie i podgląd odtwarzanych wiadomości email.
   - Granularne odtwarzanie baz danych Microsoft SQL.
   - Możliwość granularnego odtwarzania witryn i plików Microsoft SharePoint.
   - Odtwarzanie kontrolerów domeny Microsoft Active Directory.
   - Granularne odtwarzanie baz danych Oracle.

5. Dodatkowe wymagania związane ochroną danych:
   - Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń.

6. Wymagania co do modelu licencjonowania rozwiązania:
   - Możliwość zakupu licencji subskrypcyjnych w okresie do 30.06.2026.
   - Model licencjonowania oparty na maszynach fizycznych i hostach – brak limitów na chronioną ilość danych, maszyn wirtualnych i aplikacji).

3. Usługa szkolenia: "Cyberbezpieczny samorząd" dla kadry administracyjnej, informatycznej oraz zarządzającej.

Wykonawca ma zapewnić dostęp do cyklu szkoleń dotyczących szeroko rozumianego cyberbezpieczeństwa
Dostęp dla 28 użytkowników.
Szkolenia powinny zawierać moduły szkoleniowe zakończone testem,
Każdy moduł powinien zawierać pytania kontrolne, które na bieżąco - w trakcie szkoleń – mają zwracać uwagę szkolących się na najważniejsze zagadnienia w danym module.

1. Wprowadzenie do bezpieczeństwa – ogólny obraz cyberbezpieczeństwa, podstawowe terminy i zagadnienia;

2. OSINT i inne metody pozyskiwania informacji o zagrożeniach – wprowadzenie do OSINT-u, przykłady podstawowych narzędzi i omówienie sposobu korzystania z nich;
3. Informacje i zagrożenia – omówienie wartości informacji w obecnym świecie, rodzaje tajemnic funkcjonujących w obrocie, wprowadzenie do budowy SZBI, podstawowe narzędzia pomocne w tworzeniu Systemu Zarządzania Bezpieczeństwem Informacji;
4. Bezpieczeństwo fizyczne – zasady fizycznego zabezpieczenia nośników informacji, opis metod stosowania zabezpieczeń technicznych i dopasowania do zagrożeń;
5. Bezpieczeństwo urządzeń mobilnych – zasady pracy z różnymi rodzajami urządzeń mobilnych, sposoby właściwego użytkowania i zabezpieczenia urządzeń;
6. Ataki i zagrożenia, rodzaje ataków na systemy teleinformatyczne – przybliżenie rodzajów ataków i sposobów myślenia cyberprzestępców, ;
7. Phishing, smishing i inne bazujące na podobnych mechanizmach ataki – analiza rodzajów ataków phishingowych, sposoby ochrony;
8. Malware, ransomware – oprogramowanie złośliwe, sposoby jego działania, metody infekcji, ograniczenie skuteczności tego typu oprogramowania;
9. Czy sprawcę można znaleźć? Trochę o informatyce śledcze – zasady zachowania po ataku, wprowadzenie do elementarnych zasad zabezpieczenia dowodów, komunikacji kryzysowej, przekazywania informacji do odpowiednich służb i instytucji;
10. Cyberhigiena. Zasady bezpiecznego postępowania w cyberświecie – omówienie zasad bezpiecznego korzystania z systemów i sieci teleinformatycznych, wypracowanie nawyków bezpiecznej pracy w cyberprzestrzeni.

Każde szkolenie powinno składać się z:
1. materiału edukacyjnego poruszającego wybrane zagadnienie,
2. testu sprawdzającego wiedzę,
3. imiennego certyfikatu potwierdzającego pozytywny wynik testu z danego obszaru.

Platforma udostępniana jest na okres nie przekraczający 30.06.2026 r. dla określonej liczby użytkowników, wskazanej przez Klienta.
Platforma powinna być dostępna w modelu SaaS (Software as a Service), czyli całość oprogramowania i sprzętu znajduje się w infrastrukturze dostarczającego szkolenie
 Dostawca szkoleń odpowiada za nadanie uprawnień administratora przedstawicielom klienta oraz całość prac związanych z utrzymaniem technicznym platformy
Raportowanie i analizy: Platforma szkoleniowa powinna oferować funkcje raportowania, które pozwalają śledzić postępy uczestników kursów, oceny, aktywność itp.
Bezpieczeństwo i dostępność: Platforma szkoleniowa , powinna zapewniać funkcje związane z bezpieczeństwem danych oraz dostępnością, aby zapewnić, że platforma jest zgodna z przepisami dotyczącymi ochrony danych i dostępności online.
Wsparcie techniczne i aktualizacje: Platforma szkoleniowa powinna oferować wsparcie techniczne oraz regularne aktualizacje, aby zapewnić płynne działanie platformy i rozwiązywanie ewentualnych problemów.
Certyfikaty: Ukończone kursy oraz zakończone aktywności dają możliwości raportowe. Możliwość uzyskanie spersonalizowanego certyfikatu ukończenia po przez platformę po skończeniu szkolenia.