Możliwość dofinansowania

Szkolenie MS 500 Microsoft 365 Security Administration

Numer usługi 2026/06/03/5395/3607140

3 200,00 PLN brutto
3 200,00 PLN netto
100,00 PLN brutto/h
100,00 PLN netto/h
261,33 PLN cena rynkowa

NTG.pl Sp. z o.o.

4,4 / 5

5 666 ocen

Łódź
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
32:00 h
07.07.2026 do 10.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, Nowy start w Małopolsce z EURESEM, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe
Grupa docelowa usługi	Szkolenie skierowane jest do administratorów IT oraz specjalistów ds. bezpieczeństwa odpowiedzialnych za zarządzanie i ochronę środowiska Microsoft 365. Przeznaczone dla osób posiadających podstawową wiedzę z zakresu administracji systemami i usługami chmurowymi, do pracowników zajmujących się ochroną danych, zgodnością z regulacjami oraz zarządzaniem bezpieczeństwem informacji w organizacji.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	03-07-2026
Forma prowadzenia usługi	stacjonarna
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Celem szkolenia jest zdobycie wiedzy i praktycznych umiejętności z zakresu zabezpieczania środowiska Microsoft 365. Uczestnicy nauczą się zarządzać tożsamością i dostępem użytkowników, wdrażać mechanizmy ochrony przed zagrożeniami oraz zabezpieczać dane i urządzenia w organizacji. Przygotowanie do monitorowania bezpieczeństwa, zarządzania zgodnością oraz stosowania narzędzi ochrony informacji i danych w środowisku chmurowym Microsoft 365.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik zarządza tożsamościami, użytkownikami i grupami w Microsoft 365/Azure AD zgodnie z zasadami bezpieczeństwa	Tworzy i usuwa konta użytkowników, przypisuje role i grupy, stosuje RBAC oraz opisuje model Zero Trust	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik konfiguruje i nadzoruje synchronizację tożsamości oraz mechanizmy ochrony haseł	Konfiguruje synchronizację katalogów (np. Azure AD Connect), analizuje status synchronizacji, wdraża polityki haseł i Identity Protection	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wdraża i zarządza kontrolą dostępu do zasobów i urządzeń	Tworzy polityki Conditional Access, zarządza dostępem urządzeń (MDM/MAM), kontroluje dostęp użytkowników zewnętrznych	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wdraża i stosuje mechanizmy ochrony informacji i danych w Microsoft 365	Konfiguruje DLP, etykiety poufności, AIP/WIP oraz szyfrowanie wiadomości i IRM	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik monitoruje, analizuje i reaguje na zagrożenia bezpieczeństwa w środowisku Microsoft 365	Korzysta z Microsoft Defender, Sentinel i Security Center, analizuje alerty, przeprowadza analizę logów i reaguje na incydenty	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

📘 Jak wygląda szkolenie?

Szkolenie prowadzone jest w sposób uporządkowany i praktyczny - składa się z trzech etapów:

- Wprowadzenie teoretyczne
- Ćwiczenia wspólne z trenerem – wykonujemy zadania krok po kroku, ucząc się na konkretnych przykładach.
- Zadania do samodzielnego wykonania – utrwalenie wiedzy.

🤝 Opieka poszkoleniowa

Po zakończeniu szkolenia zapewniamy pełną opiekę poszkoleniową:

- kontakt z trenerem
- wsparcie techniczne i merytoryczne po szkoleniu
- dodatkowe materiały i wskazówki, które pomogą wracać do kluczowych zagadnień.

PROGRAM:

Moduł 1: Zarządzanie użytkownikami i grupami:

- Koncepcje zarządzania tożsamością i dostępem
- Model Zero Trust
- Planowanie rozwiązania tożsamości i uwierzytelniania
- Konta użytkowników i role
- Zarządzanie tożsamością

Moduł 2: Synchronizacja i ochrona tożsamości:

- Planowanie synchronizacji katalogów
- Konfiguracja i zarządzanie synchronizowanymi tożsamościami
- Zarządzanie hasłami
- Azure AD Identity Protection

Moduł 3: Zarządzanie dostępem:

- Dostęp warunkowy
- Zarządzanie dostępem urządzeń
- Kontrola dostępu oparta na rolach (RBAC)
- Rozwiązania dostępu zewnętrznego

Moduł 4: Bezpieczeństwo w Microsoft 365:

- Wektory zagrożeń i naruszenia danych
- Strategia i zasady bezpieczeństwa
- Rozwiązania bezpieczeństwa dla Microsoft 365
- Secure Score

Moduł 5: Ochrona przed zagrożeniami:

- Exchange Online Protection (EOP)
- Office 365 Advanced Threat Protection
- Zarządzanie załącznikami
- Zarządzanie linkami
- Azure Advanced Threat Protection
- Microsoft Defender Advanced Threat Protection

Moduł 6: Zarządzanie zagrożeniami:

- Panel bezpieczeństwa
- Badanie zagrożeń i reagowanie
- Azure Sentinel
- Advanced Threat Analytics

Moduł 7: Bezpieczeństwo aplikacji chmurowych:

- Wdrażanie Cloud Application Security
- Wykorzystanie informacji Cloud Application Security

Moduł 8: Bezpieczeństwo aplikacji chmurowych:

- Zarządzanie aplikacjami mobilnymi (MAM)
- Zarządzanie urządzeniami mobilnymi (MDM)
- Wdrażanie usług urządzeń mobilnych
- Rejestrowanie urządzeń w MDM

Moduł 9: Ochrona informacji:

- Koncepcje ochrony informacji
- Etykiety poufności
- Azure Information Protection (AIP)
- Windows Information Protection (WIP)

Moduł 10: Zarządzanie prawami i szyfrowanie:

- Zarządzanie prawami do informacji (IRM)
- Bezpieczne rozszerzenie do poczty elektronicznej (S/MIME)
- Szyfrowanie wiadomości w usłudze Office 365

Moduł 11: Zapobieganie utracie danych:

- Zapobieganie utracie danych
- Tworzenie polityki DLP
- Dostosowywanie polityki DLP
- Tworzenie polityki DLP do ochrony dokumentów
- Wskazówki dotyczące polityk

Moduł 12: Archiwizacja i utrzymanie danych:

- Archiwizacja w Microsoft 365
- Utrzymanie danych w Microsoft 365
- Zasady utrzymywania danych w centrum zgodności Microsoft 365
- Archiwizacja i utrzymywanie danych w Exchange
- Zarządzanie zapisami w SharePoint

Moduł 13: Wyszukiwanie treści:

- Przeszukiwanie zawartości
- Badanie/analiza logów audytowych
- Zaawansowane wykrywanie elektroniczne

Moduł 14: Zgodność w Microsoft 365:

- Centrum zgodności
- Rozwiązania Compliance Center
- Budowanie „ethical walls” w Exchange Online

Test z wynikiem generowanym automatycznie.

Harmonogram

Liczba pozycji harmonogramu: 30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 30 Moduł 1: Zarządzanie użytkownikami i grupami	Zajęcia	Adam Bartosiewicz	07-07-2026	08:00	10:00	02:00
2 z 30 -	Przerwa	-	07-07-2026	10:00	10:15	00:15
3 z 30 Moduł 2: Synchronizacja i ochrona tożsamości	Zajęcia	Adam Bartosiewicz	07-07-2026	10:15	12:15	02:00
4 z 30 -	Przerwa	-	07-07-2026	12:15	12:45	00:30
5 z 30 Moduł 3: Zarządzanie dostępem - teoria	Zajęcia	Adam Bartosiewicz	07-07-2026	12:45	14:15	01:30
6 z 30 -	Przerwa	-	07-07-2026	14:15	14:30	00:15
7 z 30 Moduł 3: Zarządzanie dostępem - praktyka	Zajęcia	Adam Bartosiewicz	07-07-2026	14:30	16:00	01:30
8 z 30 Moduł 4: Bezpieczeństwo w Microsoft 365	Zajęcia	Adam Bartosiewicz	08-07-2026	08:00	10:00	02:00
9 z 30 -	Przerwa	-	08-07-2026	10:00	10:15	00:15
10 z 30 Moduł 5: Ochrona przed zagrożeniami:	Zajęcia	Adam Bartosiewicz	08-07-2026	10:15	12:15	02:00
11 z 30 -	Przerwa	-	08-07-2026	12:15	12:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 30 Moduł 6: Zarządzanie zagrożeniami	Zajęcia	Adam Bartosiewicz	08-07-2026	12:45	14:15	01:30
13 z 30 -	Przerwa	-	08-07-2026	14:15	14:30	00:15
14 z 30 Moduł 7: Bezpieczeństwo aplikacji chmurowych - teoria	Zajęcia	Adam Bartosiewicz	08-07-2026	14:30	16:00	01:30
15 z 30 Moduł 7: Bezpieczeństwo aplikacji chmurowych - praktyka	Zajęcia	Adam Bartosiewicz	09-07-2026	08:00	10:00	02:00
16 z 30 -	Przerwa	-	09-07-2026	10:00	10:15	00:15
17 z 30 Moduł 8: Bezpieczeństwo aplikacji chmurowych:	Zajęcia	Adam Bartosiewicz	09-07-2026	10:15	10:30	00:15
18 z 30 Moduł 9: Ochrona informacji	Zajęcia	Adam Bartosiewicz	09-07-2026	10:30	12:15	01:45
19 z 30 -	Przerwa	-	09-07-2026	12:15	12:45	00:30
20 z 30 Moduł 10: Zarządzanie prawami i szyfrowanie - teoria	Zajęcia	Adam Bartosiewicz	09-07-2026	12:45	14:15	01:30
21 z 30 -	Przerwa	-	09-07-2026	14:15	14:30	00:15
22 z 30 Moduł 10: Zarządzanie prawami i szyfrowanie - praktyka	Zajęcia	Adam Bartosiewicz	09-07-2026	14:30	16:00	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
23 z 30 Moduł 11: Zapobieganie utracie danych	Zajęcia	Adam Bartosiewicz	10-07-2026	08:00	10:00	02:00
24 z 30 -	Przerwa	-	10-07-2026	10:00	10:15	00:15
25 z 30 Moduł 12: Archiwizacja i utrzymanie danych	Zajęcia	Adam Bartosiewicz	10-07-2026	10:15	12:15	02:00
26 z 30 -	Przerwa	-	10-07-2026	12:15	12:45	00:30
27 z 30 Moduł 13: Wyszukiwanie treści	Zajęcia	Adam Bartosiewicz	10-07-2026	12:45	14:15	01:30
28 z 30 -	Przerwa	-	10-07-2026	14:15	14:30	00:15
29 z 30 Moduł 14: Zgodność w Microsoft 365	Zajęcia	Adam Bartosiewicz	10-07-2026	14:30	15:30	01:00
30 z 30 -	Walidacja	Adam Bartosiewicz	10-07-2026	15:30	16:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	32:00
w tym suma godzin zajęć	27:30
w tym suma godzin walidacji	00:30
w tym suma przerw	04:00
Suma godzin dydaktycznych bez przerw	37:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 200,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	3 200,00 PLN
Koszt osobogodziny brutto	100,00 PLN
Koszt osobogodziny netto	100,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	32:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Adam Bartosiewicz

Ponad 10 lat doświadczenia w prowadzeniu szkoleń IT.
Realizacja szkoleń w zakresie kompetencji cyfrowych a w szczególności produktów: Teams / SharePoint, chmura Office 365, pakietu biurowego Microsoft Office w szczególności aplikacji analitycznych. Uczy tego, że technologia daje nam niepowtarzalną szanse bycia twórczym. Trener posiada doświadczenie zdobyte nie wcześniej niż 5 lat przed datą publikacji usługi w BUR.
Wykształcenie: wyższe

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Autoryzowane materiały Microsoft w formie elektronicznej. Laboratorium on-line niezbędne do wykonywania ćwiczeń / symulacji dostępne będą dla uczestnika przez 6 miesięcy od zakończenia szkolenia.

Informacje dodatkowe

Uczestnik powinien uzyskać frekwencje w min. 80% zajęć.

Po ukończeniu szkolenia uczestnik otrzymuje certyfikat Microsoft potwierdzający zdobyte umiejętności.

Podczas szkoleń istnieje możliwość przeprowadzenia kontroli/audytu usługi przez osoby do tego upoważnione przez PARP.

Jak skorzystać z usług dofinansowanych?

- Krok 1: Założenie konta indywidualnego/instytucjonalnego w Bazie Usług Rozwojowych.
- Krok 2: Złożenie wniosku do Operatora, który rozdziela środki w Twoim województwie.
- Krok 3: Uzyskanie dofinasowania.
- Krok 4: Zapisanie na szkolenie poprzez platformę BUR.

Adres

ul. Pomorska 65

90-218 Łódź

woj. łódzkie

Piętro 3

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt

NTG.pl sp. z o.o.

E-mail ntg@ntg.edu.pl
Telefon (+48) 609 009 742