



"GLOBAL
INFORMATION
SECURITY" SPÓŁKA
Z OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ

★★★★★ 4,5 / 5

269 ocen

"Cyberbezpieczeństwo" - usługa zdalna na platformie e- Lea

Numer usługi 2025/11/04/51633/3125576

📍 zdalna

🏢 Usługa szkoleniowa

🕒 16 h

📅 05.01.2026 do 26.06.2026

1 230,00 PLN brutto

1 000,00 PLN netto

76,88 PLN brutto/h

62,50 PLN netto/h

213,44 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria

Biznes / Zarządzanie przedsiębiorstwem

Grupa docelowa usługi

Nowa usługa szkoleniowa „Cyberbezpieczeństwo” została stworzona z myślą o firmach, które priorytetowo traktują ochronę swoich informacji – zarówno w kontekście tradycyjnych zagrożeń, jak i najnowszych wyzwań, takich jak wykorzystanie sztucznej inteligencji (AI). Autorzy podjęli próbę przybliżenia tej tematyki w maksymalnie przystępny sposób.

Uczestnikami szkolenia mogą być osoby indywidualne, które chcą zrozumieć istotę zagrożeń związanych z cyberbezpieczeństwem, ocenić ryzyko aby świadomie i skutecznie przeciwdziałać tym ryzykom.

Minimalna liczba uczestników

1

Maksymalna liczba uczestników

500

Data zakończenia rekrutacji

04-01-2026

Forma prowadzenia usługi

zdalna

Liczba godzin usługi

16

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

Uczestnik usługi rozwojowej będzie przygotowany do świadomego podejmowania działań celem chronienia zasobów cyfrowych firmy i swoich prywatnych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik zna naturę zagrożeń i posiada wiedzę pozwalającą promować cyberbezpieczeństwo w swoim środowisku	Zrozumienie istoty cyberbezpieczeństwa, znajomość najgroźniejszych i najczęstszych zagrożeń, ryzyk związanych z cyberbezpieczeństwem i podstawowych zabezpieczeń zmniejszających ich wpływ lub prawdopodobieństwo ich pojawienia się.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Program „Cyberbezpieczeństwo”

1. Wprowadzenie do cyberbezpieczeństwa

- Czym jest cyberbezpieczeństwo?
- Dlaczego jest ważne w życiu codziennym i zawodowym?

2. Silne hasła i zarządzanie nimi

- Jak tworzyć bezpieczne hasła
- Korzystanie z menedżerów haseł
- Czego unikać (np. używanie tego samego hasła wszędzie)

3. Rozpoznawanie zagrożeń: phishing i oszustwa

- Jak wyglądają typowe próby wyłudzenia danych
- Jak nie dać się nabrać na fałszywe e-maile i SMS-y
- Co robić, gdy mamy podejrzenie ataku?

4. Bezpieczne korzystanie z Internetu i urządzeń

- Aktualizacje systemów i oprogramowania
- Zabezpieczanie sieci Wi-Fi
- Używanie antywirusa i zapory sieciowej (firewall)

5. Bezpieczeństwo w mediach społecznościowych i komunikatorach

- Ochrona prywatności online
- Ustawienia prywatności i bezpieczeństwa
- Unikanie nadmiernego udostępniania informacji

6. Reagowanie na incydenty i dobre praktyki na co dzień

- Co robić w przypadku podejrzenia naruszenia bezpieczeństwa
- Do kogo się zgłosić (np. dział IT)
- Codzienne nawyki wspierające cyberbezpieczeństwo

7. Testy

Usługa jest realizowana przy wykorzystaniu licencji: Licencje SaaS na 24 miesiące, Profesjonalnej Platformy Edukacyjnej e-Lea Enterprise dofinansowanej w ramach projektu "Nowa perspektywa dla BUR" nr FERS 01.03-IP.09-0019/2023

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 230,00 PLN
Koszt przypadający na 1 uczestnika netto	1 000,00 PLN
Koszt osobogodziny brutto	76,88 PLN
Koszt osobogodziny netto	62,50 PLN

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają pełny zestaw materiałów na platformie e-Lea, w tym :

1. wykłady :

- Wprowadzenie do cyberbezpieczeństwa
- • Czym jest cyberbezpieczeństwo?
- • Dlaczego jest ważne w życiu codziennym i zawodowym
- Silne hasła i zarządzanie nimi
- • Jak tworzyć bezpieczne hasła
- • Korzystanie z menedżerów haseł
- • Czego unikać
- Rozpoznawanie zagrożeń: phishing i oszustwa
- • Jak wyglądają typowe próby wyłudzenia danych
- • Jak nie dać się nabrać na fałszywe e-maile i SMS-y
- • Co robić, gdy mamy podejrzenie ataku?
- Bezpieczne korzystanie z Internetu i urządzeń
- • Aktualizacje systemów i oprogramowania
- • Zabezpieczanie sieci Wi-Fi
- • Używanie antywirusa i zapory sieciowej (firewall)
- Bezpieczeństwo w mediach społecznościowych i komunikatorach
- • Ochrona prywatności online
- • Ustawienia prywatności i bezpieczeństwa
- • Unikanie nadmiernego udostępniania informacji
- Reagowanie na incydenty i dobre praktyki na co dzień
- • Co robić w przypadku podejrzenia naruszenia bezpieczeństwa
- • Do kogo się zgłosić (np. dział IT)
- • Codzienne nawyki wspierające cyberbezpieczeństwo

1. Materiały pomocnicze rozszerzające i wyjaśniające .

2. **Egzamin końcowy:** 10 pytań testowych z obszaru objętego niniejszym szkoleniem

3. **Certyfikat i Open Badge** - cyfrowe potwierdzenie ukończenia szkolenia "Cyberbezpieczeństwo" oraz

Warunki techniczne

Wymogi techniczne dla uczestników usługi - szkolenia "Cyberbezpieczeństwo"

1. Do korzystania z Usługi Profesjonalnej Platformy Edukacyjnej e-LEA (za pomocą której udostępniane jest szkolenie "Cyberbezpieczeństwo") konieczne jest spełnienie następujących warunków technicznych przez komputer lub inne urządzenie Klienta lub Użytkownika Końcowego. Klient zawrze identyczne lub bardziej restrykcyjne wymagania techniczne dla Użytkownika Końcowego Platformy Klientkiej.

- System operacyjny: Windows 7 lub nowszy, MacOS 10.12 lub nowszy.
- Pamięć operacyjna: co najmniej 4 GB, optymalnie 8 GB i więcej; w przypadku komputerów z systemem Windows 8 lub nowszym zaleca się minimum 8 GB RAM.
- Urządzenia peryferyjne lub wbudowane: słuchawki i mikrofon (lub głośniki i mikrofon), kamera internetowa – wymagane do udziału w wykładach LIVE.
- Ekran: rozdzielczość co najmniej 1280x768.
- Miejsce na dysku: 20 MB wolnego miejsca.
- Internet: stabilne łącze o parametrach:
 - • pobieranie powyżej 512 kbps (jakość SD),
 - • pobieranie powyżej 2 Mbps (jakość HD),
 - • pobieranie i wysyłanie powyżej 10 Mbps (jakość Full HD, udział w wydarzeniach online),
 - • opóźnienie do 40 ms.
- Rekomendowane parametry internetu: pobieranie i wysyłanie od 30 Mbps, opóźnienie do 40 ms.
- Przeglądarka: aktualna wersja Chrome, Safari, Firefox lub Edge z obsługą plików audio i wideo.

- Adres e-mail: aktywny adres e-mail uczestnika.
 - Urządzenia mobilne: aplikacja e-LEA pobrana z Google Play (Android) lub App Store (iOS).
 - Karta graficzna: opcjonalna, zwiększa płynność i wydajność przy dużej liczbie grafik i filmów.
 - Karta dźwiękowa: opcjonalna; w przypadku jej braku dźwięk odtwarzany jest przez urządzenia peryferyjne lub wbudowane.
1. Usługa Profesjonalnej Platformy Edukacyjnej e-LEA jest świadczona w modelu SaaS (Software as a Service), co oznacza, że oprogramowanie platformy jest instalowane i utrzymywane w całości w ramach infrastruktury e-LEA oraz udostępniane Klientowi online.
 2. Klient w trakcie, przed i po okresie użytkowania nie nabywa jakichkolwiek praw do oprogramowania Platformy.

Kontakt



Marek Pióro

E-mail marek.pioro@globinfosec.pl

Telefon (+48) 601 131 654