



ASKREATE.COM

ASKREATE.COM

ALEKSANDRA

SKOWRONEK

★★★★★ 4,9 / 5

502 oceny

Cyberbezpieczeństwo w erze ESG i Green Deal: bezpieczna komunikacja, dane i cyfrowe środowisko pracy - szkolenie z certyfikatem kwalifikacyjnym

Numer usługi 2025/12/07/154524/3196622

📍 Jaworze / stacjonarna

🏠 Usługa szkoleniowa

🕒 18 h

📅 14.03.2026 do 15.03.2026

5 250,00 PLN brutto

5 250,00 PLN netto

291,67 PLN brutto/h

291,67 PLN netto/h

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

Szkolenie skierowane jest do:

- pracowników sektora MŚP oraz organizacji publicznych,
- specjalistów odpowiedzialnych za przetwarzanie, ochronę i archiwizację danych,
- menedżerów zespołów, koordynatorów projektów oraz osób zarządzających informacją w firmie,
- nauczycieli, trenerów i edukatorów wykorzystujących technologie cyfrowe,
- osób pracujących zdalnie lub hybrydowo, które chcą zwiększyć bezpieczeństwo swojej pracy,
- wszystkich osób chcących rozwinąć **zielone kompetencje cyfrowe**, w szczególności w zakresie bezpiecznego i zasobooszczędnego korzystania z technologii.

Szkolenie jest odpowiednie zarówno dla osób początkujących, jak i średniozaawansowanych w tematyce cyberbezpieczeństwa.

Minimalna liczba uczestników

5

Maksymalna liczba uczestników

20

Data zakończenia rekrutacji

13-03-2026

Forma prowadzenia usługi

stacjonarna

Liczba godzin usługi

18

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

Szkolenie przygotowuje do świadomego, bezpiecznego i odpowiedzialnego korzystania z technologii cyfrowych w środowisku pracy, zgodnie z wytycznymi ESG i Europejskiego Zielonego Ładu. Uczestnicy nauczą się rozpoznawać i minimalizować zagrożenia cybernetyczne, chronić dane oraz stosować praktyki cyberhigieny w pracy stacjonarnej, zdalnej i hybrydowej. Szkolenie przygotowuje do wdrażania zasobooszczędnych, ekologicznych i etycznych standardów pracy cyfrowej, wspierających rozwój zielonych kompetencji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik definiuje podstawowe pojęcia i zagrożenia z zakresu cyberbezpieczeństwa.	Uczestnik poprawnie opisuje typy cyberataków i ich konsekwencje	Test teoretyczny
Uczestnik definiuje zasady ochrony danych i bezpiecznej komunikacji w środowisku cyfrowym.	Uczestnik wskazuje dobre i złe praktyki ochrony danych.	Test teoretyczny
Uczestnik rozumie zależność między cyberbezpieczeństwem, ESG i zielonymi kompetencjami cyfrowymi.	Uczestnik wymienia elementy ESG związane z bezpieczeństwem informacji	Test teoretyczny
Uczestnik wymienia narzędzia wspierające cyberbezpieczeństwo (VPN, MFA, szyfrowanie).	Uczestnik dobiera narzędzie do określonej sytuacji.	Test teoretyczny
Uczestnik stosuje zasady tworzenia bezpiecznych haseł i konfiguracji MFA.	Uczestnik tworzy poprawny zestaw haseł zgodnie z zasadami bezpieczeństwa	Test teoretyczny
Uczestnik identyfikuje najczęściej występujące próby phishingu i ataki socjotechniczne.	Uczestnik poprawnie klasyfikuje przykładowe wiadomości jako bezpieczne lub podejrzane.	Test teoretyczny
Uczestnik stosuje praktyki cyberhigieny w pracy zdalnej i chmurowej	Uczestnik wykonuje zadania nawiązywania połączeń przy użyciu bezpiecznych narzędzi	Test teoretyczny
Uczestnik optymalizuje dane i dokumenty zgodnie z zasadami zasobooszczędnej pracy cyfrowej.	Uczestnik kompresuje, porządkuje i archiwizuje pliki zgodnie z instrukcją	Test teoretyczny
Uczestnik wykorzystuje bezpieczne i ekologiczne formy cyfrowej komunikacji	Uczestnik przygotowuje zestaw praktyk minimalizujących ryzyko i ślad cyfrowy	Test teoretyczny
Uczestnik rozumie odpowiedzialność indywidualną za bezpieczeństwo informacji w organizacji.	Uczestnik formułuje przykłady działań pracownika wpływających na poziom cyberbezpieczeństwa.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik współpracuje w budowaniu zielonego i bezpiecznego środowiska cyfrowego.	Uczestnik w pracy zespołowej identyfikuje działania wspierające kulturę bezpieczeństwa.	Test teoretyczny

Kwalifikacje

Inne kwalifikacje

Uznane kwalifikacje

Pytanie 4. Czy dokument potwierdzający uzyskanie kwalifikacji jest rozpoznawalny i uznawalny w danej branży/sektorze (czy certyfikat otrzymał pozytywne rekomendacje od co najmniej 5 pracodawców danej branży/sektorów lub związku branżowego, zrzeszającego pracodawców danej branży/sektorów)?

TAK

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa
Nazwa Podmiotu prowadzącego walidację	Fundacja My Personality Skills
Podmiot prowadzący walidację jest zarejestrowany w BUR	Tak
Nazwa Podmiotu certyfikującego	Fundacja My Personality Skills
Podmiot certyfikujący jest zarejestrowany w BUR	Tak

Program

Celem szkolenia "**Cyberbezpieczeństwo w erze ESG i Green Deal: bezpieczna komunikacja, dane i cyfrowe środowisko pracy - szkolenie z certyfikatem kwalifikacyjnym**" jest wyposażenie uczestników w wiedzę i praktyczne kompetencje z zakresu **cyberbezpieczeństwa i zrównoważonej cyfryzacji**, pozwalające na bezpieczne, odpowiedzialne i zasobooszczędne korzystanie z technologii w miejscu pracy.

Po zakończeniu szkolenia uczestnik:

Cele ogólne

- rozumie ideę cyberbezpieczeństwa w kontekście ESG, Green Deal oraz zielonych kompetencji cyfrowych,
- potrafi rozpoznawać, analizować i minimalizować współczesne cyberzagrożenia,
- wie, jak chronić dane osobowe i służbowe zgodnie z zasadami bezpieczeństwa cyfrowego,
- rozumie wpływ korzystania z technologii na środowisko i potrafi zmniejszać swój cyfrowy ślad węglowy.

Cele szczegółowe

- stosuje bezpieczne praktyki pracy zdalnej, mobilnej i hybrydowej,
- potrafi wykrywać próby phishingu, spoofingu, ataków socjotechnicznych,
- umie korzystać z chmury i komunikatorów w sposób bezpieczny i zgodny z zasadami cyfrowej higieny,
- potrafi tworzyć i zarządzać bezpiecznymi hasłami i autoryzacją dwuskładnikową,
- zna zasady bezpiecznego korzystania z AI i narzędzi automatyzujących,
- potrafi prowadzić zasobooszczędną, odpowiedzialną komunikację cyfrową (optymalizacja danych, formatów, obiegu informacji),
- zna narzędzia i dobre praktyki wspierające zgodność z ESG w obszarze cyfryzacji,
- rozumie, jak właściwa organizacja pracy cyfrowej wpływa na bezpieczeństwo i środowisko.

Zakres szkolenia i kompetencje, które nabędzie uczestnik są zielone na podstawie bazy danych ESCO – wykazu przykładowych zielonych umiejętności opracowanych przez KE w ramach klasyfikacji ESCO. Szkolenie zgodne jest z obszarami i grupami technologii wskazanymi w Regionalnej Strategii Innowacji Województwa Śląskiego 2030 oraz Programie Rozwoju Technologii Województwa Śląskiego na lata 2019-2030 tj. "Technologie informacyjne i komunikacyjne" (4.1, 4.2, 4.4, 4.6)

oraz wykazem przykładowych zielonych umiejętności opracowanych przez KE w ramach kwalifikacji ESCO.

Szkolenie: "Cyberbezpieczeństwo w erze ESG i Green Deal: bezpieczna komunikacja, dane i cyfrowe środowisko pracy - szkolenie z certyfikatem kwalifikacyjnym" prowadzi do nabycia kwalifikacji: **"Specjalista ds. cyberbezpieczeństwa z elementami zrównoważonego rozwoju"**.

Uczestnik szkolenia nabędzie **zielone i cyfrowe kompetencje** m.in. tj.

- obszar technologiczny: technologie informacyjne i komunikacyjne - zarządzanie wiedzą zaawansowane bazy danych, wspierające narzędzia komunikacji urządzeń
- Angażuje innych w zachowania przyjazne dla środowiska,
- Promuje odpowiedzialne zachowania konsumenckie i świadomość środowiskową Dostosowuje umiejętności do rynku pracy dotyczące transformacji ekologicznej.

Szkolenie będzie trwało 2 dni i będzie miało formę głównie warsztatową. Zarówno pierwszy jak i drugi dzień szkoleniowy będzie trwać 9 godzin dydaktycznych. Na każdy dzień szkoleniowy przypada 15 min przerwy kawowej i 30 min przerwy obiadowej. Przerwy wliczone są w czas trwania usługi.

Szkolenie składa się z części teoretycznej i części praktycznej, które opisane są w harmonogramie szkolenia jako część warsztatowa.

Warunki organizacyjne:

Stanowiska pracy: Każdy z Uczestników będzie miał zapewniony sprzęt komputerowy z odpowiednim oprogramowaniem. Istnieje możliwość pracy na własnym sprzęcie komputerowym (laptop, tablet). Praca będzie odbywała się indywidualnie (nie w grupach).

Program szkolenia:

MODUŁ 1. Wprowadzenie do cyberbezpieczeństwa i ESG

- Nowoczesne cyberbezpieczeństwo – definicje, obszary, najczęstsze zagrożenia.
- Rola bezpieczeństwa cyfrowego w strategiach ESG i Europejskim Zielonym Ładzie.
- Zielone kompetencje cyfrowe: przegląd GreenComp i wymagań kompetencyjnych UE.
- Cyfrowy ślad węglowy – jak działania w sieci wpływają na środowisko?
- Bezpieczeństwo + ekologia + efektywność: zintegrowane podejście do pracy cyfrowej.

MODUŁ 2. Ochrona danych i informacji w praktyce

- Ochrona danych osobowych i służbowych w kontekście cyberzagrożeń.
- Zasady bezpiecznego przetwarzania danych zgodnie z RODO i ESG.
- Tworzenie bezpiecznych haseł, menedżery haseł, MFA (uwierzytelnianie wieloskładnikowe).
- Zasobooszczędne zarządzanie danymi: minimalizacja, archiwizacja, odpowiedzialne formaty.
- Kryteria oceny wiarygodności źródeł i informacji.

MODUŁ 3. Bezpieczna komunikacja cyfrowa w organizacji

- Cyberhigiena – praktyki bezpiecznej komunikacji mailowej, chmurowej i mobilnej.
- Wykrywanie phishingu, spoofingu, ataków socjotechnicznych (ćwiczenia, przykłady).
- Ochrona komunikacji w Teams/Zoom/Meet i zasady bezpiecznej pracy z plikami.
- Zasobooszczędna komunikacja: optymalizacja formatów, kompresja, eliminacja „cyfrowego bałaganu”.
- Praca zdalna i hybrydowa – bezpieczne łącza, VPN, szyfrowanie.

MODUŁ 4. Narzędzia i aplikacje wspierające cyberbezpieczeństwo

- Przegląd narzędzi: antywirusy, firewalle, VPN, monitorowanie aktywności.
- Cyberbezpieczne korzystanie z AI: prywatność, dane wejściowe, ryzyka.
- Jak ograniczać ryzyko korzystania z narzędzi chmurowych?
- Wdrażanie zielonych praktyk w codziennej pracy z technologią.
- Tworzenie indywidualnej checklisty bezpieczeństwa.

MODUŁ 5. Budowanie kultury cyberbezpieczeństwa w organizacji

- Budowanie nawyków cyberbezpiecznej pracy – mikrointerwencje.
- Co powinien robić użytkownik, a co organizacja?
- Rola liderów w bezpieczeństwie cyfrowym i polityce ESG.
- Przykłady naruszeń bezpieczeństwa i dobrych praktyk z polskich i europejskich organizacji.
- Plan indywidualny uczestnika: jak wdrożyć wiedzę po szkoleniu?

Harmonogram

Liczba przedmiotów/zajęć: 23

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 23 Wprowadzenie do zielonych kompetencji, cyberbezpieczeństwa i ESG	Małgorzata Lech	14-03-2026	09:00	09:30	00:30
2 z 23 Cyfrowy ślad węglowy – jak działania w sieci wpływają na środowisko	Małgorzata Lech	14-03-2026	09:30	10:00	00:30
3 z 23 Bezpieczeństwo + ekologia + efektywność: zintegrowane podejście do pracy cyfrowej.	Małgorzata Lech	14-03-2026	10:00	11:00	01:00
4 z 23 Przerwa	Małgorzata Lech	14-03-2026	11:00	11:15	00:15
5 z 23 Ochrona danych osobowych i służbowych w kontekście cyberzagrożeń.	Małgorzata Lech	14-03-2026	11:15	12:00	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 23 Zasady bezpiecznego przetwarzania danych zgodnie z RODO i ESG	Małgorzata Lech	14-03-2026	12:00	12:30	00:30
7 z 23 • Tworzenie bezpiecznych haseł, menedżery haseł, MFA (uwierzytelnianie wieloskładnikowe)	Małgorzata Lech	14-03-2026	12:30	13:00	00:30
8 z 23 Przerwa obiadowa	Małgorzata Lech	14-03-2026	13:00	13:30	00:30
9 z 23 Zasobooszczędne zarządzanie danymi: minimalizacja, archiwizacja, odpowiedzialne formaty. Kryteria oceny wiarygodności źródeł i informacji.	Małgorzata Lech	14-03-2026	13:30	14:00	00:30
10 z 23 Cyberhigiena – praktyki bezpiecznej komunikacji mailowej, chmurowej i mobilnej	Małgorzata Lech	14-03-2026	14:00	14:30	00:30
11 z 23 Wykrywanie phishingu, spoofingu, ataków socjotechnicznych (ćwiczenia, przykłady).	Małgorzata Lech	14-03-2026	14:30	15:00	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 23 Ochrona komunikacji w Teams/Zoom/Meet i zasady bezpiecznej pracy z plikami. Praca zdalna i hybrydowa – bezpieczne łącza, VPN, szyfrowanie.	Małgorzata Lech	14-03-2026	15:00	15:45	00:45
13 z 23 Narzędzia i aplikacje wspierające cyberbezpieczeństwo: antywirusy, firewalle, VPN, monitorowanie aktywności	Małgorzata Lech	15-03-2026	09:00	09:30	00:30
14 z 23 Wdrażanie zielonych praktyk w codziennej pracy z technologią. Tworzenie indywidualnej checklisty bezpieczeństwa. Ćwiczenia	Małgorzata Lech	15-03-2026	09:30	10:30	01:00
15 z 23 Budowanie kultury cyberbezpieczeństwa w organizacji	Małgorzata Lech	15-03-2026	10:30	11:00	00:30
16 z 23 Przerwa	Małgorzata Lech	15-03-2026	11:00	11:15	00:15
17 z 23 Budowanie nawyków cyberbezpiecznej pracy – mikrointerwencje . Co powinien robić użytkownik, a co organizacja?	Małgorzata Lech	15-03-2026	11:15	12:00	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
18 z 23 Rola liderów w bezpieczeństwie cyfrowym i polityce ESG. Przykłady naruszeń bezpieczeństwa i dobrych praktyk z polskich i europejskich organizacji.	Małgorzata Lech	15-03-2026	12:00	13:00	01:00
19 z 23 Przerwa obiadowa	Małgorzata Lech	15-03-2026	13:00	13:30	00:30
20 z 23 • Wykrywanie phishingu, spoofingu, ataków socjotechnicznych (ćwiczenia, przykłady).	Małgorzata Lech	15-03-2026	13:30	14:00	00:30
21 z 23 Cyberbezpieczne korzystanie z AI: prywatność, dane wejściowe, ryzyka. Jak ograniczać ryzyko korzystania z narzędzi chmurowych	Małgorzata Lech	15-03-2026	14:00	14:30	00:30
22 z 23 Walidacja szkolenia - test teoretyczny	-	15-03-2026	14:30	15:15	00:45
23 z 23 Ewaluacja szkolenia, podsumowanie, zakończenie szkolenia	Małgorzata Lech	15-03-2026	15:15	15:45	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 250,00 PLN
Koszt przypadający na 1 uczestnika netto	5 250,00 PLN
Koszt osobogodziny brutto	291,67 PLN
Koszt osobogodziny netto	291,67 PLN
W tym koszt walidacji brutto	200,00 PLN
W tym koszt walidacji netto	200,00 PLN
W tym koszt certyfikowania brutto	200,00 PLN
W tym koszt certyfikowania netto	200,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Małgorzata Lech

Małgorzata Lech – Certyfikowany Trener i Szkoleniowiec, przedsiębiorczyni oraz CEO dwóch polskich spółek. Coach z międzynarodową akredytacją ACC ICF, Master of Business English i wykładowca akademicki. W swojej pracy łączy wiedzę psychologiczną, doświadczenie biznesowe i narzędzia rozwojowe, wspierając uczestników w rozwijaniu kompetencji przyszłości zgodnych z wytycznymi ESG i zielonej transformacji. Specjalizuje się w szkoleniach rozwijających kluczowe zielone kompetencje, takie jak odpowiedzialna komunikacja, cyfrowa świadomość środowiskowa, etyczne korzystanie z technologii oraz zasobooszczędne zarządzanie informacją. Szczególnym obszarem jej działań jest cyberbezpieczeństwo, obejmujące bezpieczne praktyki pracy cyfrowej, ochronę danych, przeciwdziałanie zagrożeniom w sieci oraz edukację z zakresu ochrony małoletnich online. Pokazuje, jak łączyć bezpieczeństwo cyfrowe z ekologicznym podejściem do korzystania z technologii i minimalizowaniem cyfrowego śladu węglowego. Pracuje z liderami, nauczycielami, dyrektorami szkół i przedsiębiorcami, wspierając ich w rozwijaniu kompetencji z obszaru efektywności osobistej, komunikacji międzygeneracyjnej, budowania relacji, zarządzania zespołami oraz budowania marki osobistej i strategii sprzedaży. W przeciągu ostatnich 5 lat przepracowała ponad 500 godzin, prowadząc warsztaty i procesy rozwojowe dla biznesu oraz instytucji publicznych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy z uczestników otrzyma:

- materiały w wersji elektronicznej;
- ćwiczenia oraz skrypty, materiały autorskie, opracowane przez wykładowców-praktyków,
- certyfikat potwierdzający zdobyte kwalifikacje i pozyskane umiejętności,
- niezbędne materiały biurowe.

Stanowiska pracy będą wyposażone w sprzęt komputerowy.

Warunki uczestnictwa

Szkolenie zostanie zrealizowane w przypadku zebrania się grupy min. 5-osobowej.

Aby wziąć udział w szkoleniu należy skontaktować się do **1-go marca 2026 r.** z organizatorem szkolenia drogą mailową na adres info@aleksandraskowronek.pl bądź telefonicznie pod numerem +48 517 555 871 w kwestii zapewnienia miejsca dla uczestnika szkolenia.

Informacje dodatkowe

Szkolenie realizowane jest w godzinach dydaktycznych. Przerwy są wliczone w czas trwania usługi. Walidacja jest wliczona w czas trwania usługi.

Warunkiem ukończenia szkolenia jest obecność w 80% czasu szkolenia.

Zakres szkolenia i kompetencje, które nabędzie uczestnik są zielone na podstawie bazy danych ESCO - wykazu przykładowych zielonych umiejętności opracowanych przez Komisję Europejską w ramach klasyfikacji ESCO.

Niniejsza karta usługi stanowi własność intelektualną firmy ASkreate.com Aleksandra Skowronek.

Karta niniejszej usługi rozwojowej została przygotowana zgodnie z obowiązującym Regulaminem Bazy Usług Rozwojowych.

Usługa zwolniona jest ze stawki VAT na podstawie par. 3 ust. 1 pkt 14 Rozporządzenie Ministra Finansów z dnia 20.12.2013r. w sprawie zwolnień od podatków i usług oraz warunków stosowania tych zwolnień, w przypadku gdy udział w usłudze jest finansowany co najmniej w 70% ze środków publicznych.

Adres

ul. Turystyczna 204

43-384 Jaworze

woj. śląskie

Sala szkoleniowa w SPA HOTEL JAWOR w Jaworze

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

ALEKSANDRA SKOWRONEK

E-mail info@aleksandraskowronek.pl

Telefon (+48) 517 555 871

