

Załącznik nr 1

Mogielnica miejscowość, dnia 10.09.2025 r

**FB.271.5.2025**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest:

* 1. Szkolenia z zakresu cyberbezpieczeństwa dla kierownictwa i pracowników Urzędu Gminy i Miasta w Mogielnicy
	2. Szkolenia z zakresu cyberbezpieczeństwa dla kierownictwa i pracowników Miejsko-Gminnego Ośrodka Pomocy Społecznej w Mogielnicy
	3. Szkolenia z zakresu cyberbezpieczeństwa dla kierownictwa i pracowników w Zespole Szkół Ogólnokształcących w Mogielnicy nr 1
	4. Szkolenia z zakresu cyberbezpieczeństwa dla kierownictwa i pracowników w Publicznej Szkole Podstawowej nr 2 w Mogielnicy
	5. Szkolenia z zakresu cyberbezpieczeństwa dla kierownictwa i pracowników w Publicznej Szkole Podstawowej w Michałowicach
	6. Szkolenia z zakresu cyberbezpieczeństwa dla kierownictwa i pracowników w Publicznej Szkole Podstawowej w Borowem
	7. Szkolenie z zakresu bezpieczeństwa informacji i funkcjonowania SZBI dla kierownictwa i pracowników Urzędu Gminy i Miasta w Mogielnicy i Jednostek Organizacyjnych
	8. Szkolenie dla kierownictwa Urzędu Gminy i Miasta i jednostek organizacyjnych z zakresu Podstaw prawnych cyberbezpieczeństwa, Wymogów wynikających z KRI, uoKSC i RODO, Zarządzanie ryzykiem w bezpieczeństwie informacji i obszarach technicznych
	9. Przeprowadzenie testów socjotechnicznych dla pracowników Urzędu Gminy i Miasta w Mogielnicy i jednostek organizacyjnych wraz ze szkoleniem i omówieniem wyników testów
1. W ramach zadania pn. Szkolenia z zakresu cyberbezpieczeństwa dla kierownictwa i pracowników Urzędu Gminy i Miasta w Mogielnicy plus przekazanie materiałów na nośniki danych 2 sztuki należy wykonać poszczególne czynności:
	1. Przeprowadzić dwa dwudniowe stacjonarne szkolenia dla 28 Pracowników w wyznaczonym przez obie strony dogodnym terminie.
	2. Czas szkolenia powinien być nie krótszy niż 3h zegarowe, nie powinny jednak przekroczyć 6h zegarowych.
	3. Pierwszy termin w 2025 nie później niż do 31.10.2025
	4. Drugi termin w 2026 nie później niż do 30.04.2026
	5. Wystawić imienne certyfikaty dla uczestników szkolenia
	6. Szkolenie powinno zawierać minimum następujące elementy:
		* 1. Wstęp do cyberbezpieczeństwa
				1. Przepisy prawne, z uwzględnieniem KRI, UKSC oraz RODO
				2. Podstawowe narzędzia cyberbezpieczeństwa
				3. Z czego powinien składać się skuteczny system cyberbezpieczeństwa
				4. Jak go zbudować?
				5. ABC higieny pracy w cyberprzestrzeni
			2. Bezpieczeństwo informacji – czym jest bezpieczeństwo informacji i jak nim zarządzać
			3. Rodzaje zagrożeń
				1. Prezentacja z wykorzystanie symulatora zagrożeń internetowych
			4. Ransomware
				1. Ransomware jako najczęstszy rodzaj ataków na firmy i instytucje
				2. Jak się chronić i na co zwracać uwagę, aby nie paść ofiarą cyberprzestępców
			5. Phishing jak działa i na co zwracać uwagę, jak się przed nim chronić
				1. Przykłady zagrożeń związanych z Phishingem
				2. Kampanie Phishingowe
			6. Zasady bezpieczeństwa przy korzystaniu z poczty elektronicznej, SPAM i podstawy prawne
			7. Zasady bezpieczeństwa przy korzystaniu z internetu,
			8. Portale społecznościowe
				1. Przykłady oszustw stosowane na portalach społecznościowych.
				2. Wizerunek organizacji i własny w sieci – dlaczego należy zwracać uwagę na umieszczane tam informacje,
				3. Zasady świadomego korzystania z portali społecznościowych.
			9. incydenty
				1. jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem,
				2. zasady postępowania z incydentami,
			10. przegląd przypadków naruszeń bezpieczeństwa
2. W ramach zadania pn. Szkolenia z zakresu cyberbezpieczeństwa dla kierownictwa i pracowników Miejsko-Gminnego Ośrodka Pomocy Społecznej w Mogielnicy należy wykonać poszczególne czynności:
	1. Przeprowadzić dwa dwudniowe stacjonarne szkolenia dla 5 Pracowników w wyznaczonym przez obie strony dogodnym terminie.
	2. Czas szkolenia powinien być nie krótszy niż 3h zegarowe, nie powinien jednak przekroczyć 6h zegarowych.
	3. Pierwszy termin w 2025 nie później niż do 31.10.2025
	4. Drugi termin w 2026 nie później niż do 30.04.2026
	5. Wystawić imienne certyfikaty dla uczestników szkolenia
	6. Szkolenie powinno zawierać minimum następujące elementy:
		* 1. Wstęp do cyberbezpieczeństwa
				1. Przepisy prawne, z uwzględnieniem KRI, UKSC oraz RODO
				2. Podstawowe narzędzia cyberbezpieczeństwa
				3. Z czego powinien składać się skuteczny system cyberbezpieczeństwa
				4. Jak go zbudować?
				5. ABC higieny pracy w cyberprzestrzeni
			2. Bezpieczeństwo informacji – czym jest bezpieczeństwo informacji i jak nim zarządzać
			3. Rodzaje zagrożeń
				1. Prezentacja z wykorzystanie symulatora zagrożeń internetowych
			4. Ransomware
				1. Ransomware jako najczęstszy rodzaj ataków na firmy i instytucje
				2. Jak się chronić i na co zwracać uwagę, aby nie paść ofiarą cyberprzestępców
			5. Phishing jak działa i na co zwracać uwagę, jak się przed nim chronić
				1. Przykłady zagrożeń związanych z Phishingem
				2. Kampanie Phishingowe
			6. Zasady bezpieczeństwa przy korzystaniu z poczty elektronicznej, SPAM i podstawy prawne
			7. Zasady bezpieczeństwa przy korzystaniu z internetu,
			8. Portale społecznościowe
				1. Przykłady oszustw stosowane na portalach społecznościowych.
				2. Wizerunek organizacji i własny w sieci – dlaczego należy zwracać uwagę na umieszczane tam informacje,
				3. Zasady świadomego korzystania z portali społecznościowych.
			9. incydenty
				1. jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem,
				2. zasady postępowania z incydentami,
			10. przegląd przypadków naruszeń bezpieczeństwa
3. W ramach zadania pn. Szkolenia z zakresu cyberbezpieczeństwa dla kierownictwa i pracowników w Zespole Szkół Ogólnokształcących w Mogielnicy nr 1 należy wykonać poszczególne czynności:
	1. Przeprowadzić dwa dwudniowe stacjonarne szkolenia dla 13 Pracowników w wyznaczonym przez obie strony dogodnym terminie.
	2. Czas szkolenia powinien być nie krótszy niż 3h zegarowe, nie powinien jednak przekroczyć 6h zegarowych.
	3. Pierwszy termin w 2025 nie później niż do 01.12.2025
	4. Drugi termin w 2026 nie później niż do 30.04.2026
	5. Wystawić imienne certyfikaty dla uczestników szkolenia
	6. Szkolenie powinno zawierać minimum następujące elementy:
		* 1. Wstęp do cyberbezpieczeństwa
				1. Przepisy prawne, z uwzględnieniem KRI, UKSC oraz RODO
				2. Podstawowe narzędzia cyberbezpieczeństwa
				3. Z czego powinien składać się skuteczny system cyberbezpieczeństwa
				4. Jak go zbudować?
				5. ABC higieny pracy w cyberprzestrzeni
			2. Bezpieczeństwo informacji – czym jest bezpieczeństwo informacji i jak nim zarządzać
			3. Rodzaje zagrożeń
				1. Prezentacja z wykorzystanie symulatora zagrożeń internetowych
			4. Ransomware
				1. Ransomware jako najczęstszy rodzaj ataków na firmy i instytucje
				2. Jak się chronić i na co zwracać uwagę, aby nie paść ofiarą cyberprzestępców
			5. Phishing jak działa i na co zwracać uwagę, jak się przed nim chronić
				1. Przykłady zagrożeń związanych z Phishingem
				2. Kampanie Phishingowe
			6. Zasady bezpieczeństwa przy korzystaniu z poczty elektronicznej, SPAM i podstawy prawne
			7. Zasady bezpieczeństwa przy korzystaniu z internetu,
			8. Portale społecznościowe
				1. Przykłady oszustw stosowane na portalach społecznościowych.
				2. Wizerunek organizacji i własny w sieci – dlaczego należy zwracać uwagę na umieszczane tam informacje,
				3. Zasady świadomego korzystania z portali społecznościowych.
			9. incydenty
				1. jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem,
				2. zasady postępowania z incydentami,
			10. przegląd przypadków naruszeń bezpieczeństwa
4. W ramach zadania pn. Szkolenia z zakresu cyberbezpieczeństwa dla kierownictwa i pracowników w Publicznej Szkole Podstawowej nr 2 w Mogielnicy należy wykonać poszczególne czynności:
	1. Przeprowadzić dwa dwudniowe stacjonarne szkolenia dla 30 Pracowników w wyznaczonym przez obie strony dogodnym terminie.
	2. Czas szkolenia powinien być nie krótszy niż 3h zegarowe, nie powinien jednak przekroczyć 6h zegarowych.
	3. Pierwszy termin w 2025 nie później niż do 01.12.2025
	4. Drugi termin w 2026 nie później niż do 30.04.2026
	5. Wystawić imienne certyfikaty dla uczestników szkolenia
	6. Szkolenie powinno zawierać minimum następujące elementy:
		* 1. Wstęp do cyberbezpieczeństwa
				1. Przepisy prawne, z uwzględnieniem KRI, UKSC oraz RODO
				2. Podstawowe narzędzia cyberbezpieczeństwa
				3. Z czego powinien składać się skuteczny system cyberbezpieczeństwa
				4. Jak go zbudować?
				5. ABC higieny pracy w cyberprzestrzeni
			2. Bezpieczeństwo informacji – czym jest bezpieczeństwo informacji i jak nim zarządzać
			3. Rodzaje zagrożeń
				1. Prezentacja z wykorzystanie symulatora zagrożeń internetowych
			4. Ransomware
				1. Ransomware jako najczęstszy rodzaj ataków na firmy i instytucje
				2. Jak się chronić i na co zwracać uwagę, aby nie paść ofiarą cyberprzestępców
			5. Phishing jak działa i na co zwracać uwagę, jak się przed nim chronić
				1. Przykłady zagrożeń związanych z Phishingem
				2. Kampanie Phishingowe
			6. Zasady bezpieczeństwa przy korzystaniu z poczty elektronicznej, SPAM i podstawy prawne
			7. Zasady bezpieczeństwa przy korzystaniu z internetu,
			8. Portale społecznościowe
				1. Przykłady oszustw stosowane na portalach społecznościowych.
				2. Wizerunek organizacji i własny w sieci – dlaczego należy zwracać uwagę na umieszczane tam informacje,
				3. Zasady świadomego korzystania z portali społecznościowych.
			9. incydenty
				1. jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem,
				2. zasady postępowania z incydentami,
			10. przegląd przypadków naruszeń bezpieczeństwa
5. W ramach zadania pn. Szkolenia z zakresu cyberbezpieczeństwa dla kierownictwa i pracowników w Publicznej Szkole Podstawowej w Michałowicach należy wykonać poszczególne czynności:
	1. Przeprowadzić dwa dwudniowe stacjonarne szkolenia dla 10 Pracowników w wyznaczonym przez obie strony dogodnym terminie.
	2. Czas szkolenia powinien być nie krótszy niż 3h zegarowe, nie powinien jednak przekroczyć 6h zegarowych.
	3. Pierwszy termin w 2025 nie później niż do 01.12.2025
	4. Drugi termin w 2026 nie później niż do 30.04.2026
	5. Wystawić imienne certyfikaty dla uczestników szkolenia
	6. Szkolenie powinno zawierać minimum następujące elementy:
		* 1. Wstęp do cyberbezpieczeństwa
				1. Przepisy prawne, z uwzględnieniem KRI, UKSC oraz RODO
				2. Podstawowe narzędzia cyberbezpieczeństwa
				3. Z czego powinien składać się skuteczny system cyberbezpieczeństwa
				4. Jak go zbudować?
				5. ABC higieny pracy w cyberprzestrzeni
			2. Bezpieczeństwo informacji – czym jest bezpieczeństwo informacji i jak nim zarządzać
			3. Rodzaje zagrożeń
				1. Prezentacja z wykorzystanie symulatora zagrożeń internetowych
			4. Ransomware
				1. Ransomware jako najczęstszy rodzaj ataków na firmy i instytucje
				2. Jak się chronić i na co zwracać uwagę, aby nie paść ofiarą cyberprzestępców
			5. Phishing jak działa i na co zwracać uwagę, jak się przed nim chronić
				1. Przykłady zagrożeń związanych z Phishingem
				2. Kampanie Phishingowe
			6. Zasady bezpieczeństwa przy korzystaniu z poczty elektronicznej, SPAM i podstawy prawne
			7. Zasady bezpieczeństwa przy korzystaniu z internetu,
			8. Portale społecznościowe
				1. Przykłady oszustw stosowane na portalach społecznościowych.
				2. Wizerunek organizacji i własny w sieci – dlaczego należy zwracać uwagę na umieszczane tam informacje,
				3. Zasady świadomego korzystania z portali społecznościowych.
			9. incydenty
				1. jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem,
				2. zasady postępowania z incydentami,
			10. przegląd przypadków naruszeń bezpieczeństwa
6. W ramach zadania pn. Szkolenia z zakresu cyberbezpieczeństwa dla kierownictwa i pracowników w Publicznej Szkole Podstawowej w Borowem należy wykonać poszczególne czynności:
	1. Przeprowadzić dwa dwudniowe stacjonarne szkolenia dla 5 Pracowników w wyznaczonym przez obie strony dogodnym terminie.
	2. Czas szkolenia powinien być nie krótszy niż 3h zegarowe, nie powinien jednak przekroczyć 6h zegarowych.
	3. Pierwszy termin w 2025 nie później niż do 01.12.2025
	4. Drugi termin w 2026 nie później niż do 30.04.2026
	5. Wystawić imienne certyfikaty dla uczestników szkolenia
	6. Szkolenie powinno zawierać minimum następujące elementy:
		* 1. Wstęp do cyberbezpieczeństwa
				1. Przepisy prawne, z uwzględnieniem KRI, UKSC oraz RODO
				2. Podstawowe narzędzia cyberbezpieczeństwa
				3. Z czego powinien składać się skuteczny system cyberbezpieczeństwa
				4. Jak go zbudować?
				5. ABC higieny pracy w cyberprzestrzeni
			2. Bezpieczeństwo informacji – czym jest bezpieczeństwo informacji i jak nim zarządzać
			3. Rodzaje zagrożeń
				1. Prezentacja z wykorzystanie symulatora zagrożeń internetowych
			4. Ransomware
				1. Ransomware jako najczęstszy rodzaj ataków na firmy i instytucje
				2. Jak się chronić i na co zwracać uwagę, aby nie paść ofiarą cyberprzestępców
			5. Phishing jak działa i na co zwracać uwagę, jak się przed nim chronić
				1. Przykłady zagrożeń związanych z Phishingem
				2. Kampanie Phishingowe
			6. Zasady bezpieczeństwa przy korzystaniu z poczty elektronicznej, SPAM i podstawy prawne
			7. Zasady bezpieczeństwa przy korzystaniu z internetu,
			8. Portale społecznościowe
				1. Przykłady oszustw stosowane na portalach społecznościowych.
				2. Wizerunek organizacji i własny w sieci – dlaczego należy zwracać uwagę na umieszczane tam informacje,
				3. Zasady świadomego korzystania z portali społecznościowych.
			9. incydenty
				1. jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem,
				2. zasady postępowania z incydentami,
			10. przegląd przypadków naruszeń bezpieczeństwa
7. W ramach zadania pn. Szkolenie z zakresu bezpieczeństwa informacji i funkcjonowania SZBI dla kierownictwa i pracowników Urzędu Gminy i Miasta w Mogielnicy i Jednostek Organizacyjnych należy wykonać poszczególne czynności:
	1. Przeprowadzić stacjonarne szkolenia dla 10 Pracowników w wyznaczonym przez obie strony dogodnym terminie.
	2. Czas szkolenia powinien być nie krótszy niż 3h zegarowe, nie powinien jednak przekroczyć 6h zegarowych.
	3. Pierwszy termin w 2025 nie później niż do niż do 01.12.2025
	4. Drugi termin w 2026 nie później niż do 30.04.2026
	5. Wystawić imienne certyfikaty dla uczestników szkolenia
8. W ramach zadania pn. Szkolenie dla kierownictwa Urzędu Gminy i Miasta w Mogielnicy i jednostek organizacyjnych z zakresu Podstaw prawnych cyberbezpieczeństwa, Wymogów wynikających z KRI, uoKSC i RODO, Zarządzanie ryzykiem w bezpieczeństwie informacji i obszarach technicznych należy wykonać poszczególne czynności:
	1. Przeprowadzić stacjonarne szkolenia dla 10 Pracowników w wyznaczonym przez obie strony dogodnym terminie.
	2. Czas szkolenia powinien być nie krótszy niż 3h zegarowe, nie powinien jednak przekroczyć 6h zegarowych.
	3. Pierwszy termin w 2025 nie później niż do niż do 01.12.2025
	4. Drugi termin w 2026 nie później niż do 30.04.2026
	5. Wystawić imienne certyfikaty dla uczestników szkolenie
	6. Szkolenie powinno zawierać minimum następujące elementy:
		1. **Podstawowe informacje o obecnej sytuacji rynkowej powiązanej z tematyką cyberbezpieczeństwa**
		2. **Omówienie światowych standardów i norm w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji**
		3. **Omówienie zaawansowanych strategii ochrony organizacji**
		4. **Regulacje prawne i compliance**
9. W ramach zadania pn. Przeprowadzenie testów socjotechnicznych dla pracowników Urzędu Gminy i Miasta i jednostek organizacyjnych wraz ze szkoleniem i omówieniem wyników testów należy wykonać poszczególne czynności:
	1. Przeprowadzić kontrolowany atak hackerski z wykorzystaniem technik socjotechnicznych oraz wykorzystaniem fałszywych wiadomości e-mail
	2. Pierwszy termin w 2025 nie później niż do niż do 01.12.2025
	3. Drugi termin w 2026 nie później niż do 30.04.2026
	4. Sporządzić raport z przeprowadzonych testów wraz z omówieniem ich z Zarządem Miasta i Gminy.
	5. W przypadku negatywnego wyniku testu, przeprowadzić stacjonarne szkolenie w siedzibie Zamawiającego z pracownikami w celu instruktarzu postępowania oraz zapobieganiu występowania podobnych zdarzeń w przyszłości
	6. Wystawienia imiennych certyfikatów uczestnikom szkolenia