**Załącznik nr 1I do FORMULARZA OFERTOWEGO**

**Parametry techniczne i wyposażenie**

**CZĘŚĆ IX –szkolenia dla pracowników z zakresu cyberbezpieczeństwa**

WYPEŁNIA WYKONAWCA:

Dane Wykonawcy (nazwa, adres) : …………………………………………………………………………………….

Oferuję wykonanie szkolenia dla pracowników z zakresu cyberbezpieczeństwa.

UWAGA:

Kolumny nr 3 pt. „Potwierdzenie spełnienia wymagań TAK/NIE” należy wypełnić stosując słowa TAK lub NIE.

W przypadku, gdy Wykonawca w którejkolwiek z pozycji wpisze słowa „NIE” lub zaoferuje niższe wartości niż wymagane, oferta zostanie odrzucona, jako że jej treść jest niezgodna z warunkami zamówienia (art. 226 ust. 1 pkt 5 ustawy Pzp).

**„Dostawa urządzeń i oprogramowania wraz z  przeprowadzeniem audytu cyberbezpieczeństwa wraz ze szkoleniami dla pracowników z zakresu cyberbezpieczeństwa w ramach realizacji projektu Cyfrowa Gmina przez Gminę Ząbkowice Śląskie” z podziałem na 9 zadań/ części. ”**

W ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest do wykonania usługi zgodnej z poniższymi warunkami.

Potwierdzenie spełniania poniższych wymagań:

| Zakres wymagania | Wymaganie / Dokument | Potwierdzenie spełnienia wymagań  TAK/NIE |
| --- | --- | --- |

|  |  |  |
| --- | --- | --- |
| **Nazwa** | **Minimalne wymagania dla szkolenia** | |
| **Typ** | Szkolenie zdalne dla pracowników Urzędu z zakresu cyberbezpieczeństwa | [….] |
| **Program szkolenia** | 1. Czym jest cyberbezpieczeństwo. 2. Podstawowe przedstawienie zagadnienia cyberbezpieczenstwa 3. Przedstawienie zagrożeń, które czyhają na nas w sieci (rodzaje zagrożeń i ich konsekwencje) 4. Opis i wymagania normy ISO/IEC 27001 5. Dlaczego wiedza o cyberbezpieczeństwie jest konieczna? 6. Sposoby ochrony kont i danych przed potencjalnym zagrożeniem. 7. Częsta zmiana haseł, czy ustalanie ich odpowiedniej trudności a co za tym idzie programy pomagające w tym (np. keypas) 8. Logowanie w sieci. 9. Opis Certyfikatów stron internetowych. 10. Darmowe WiFi i automatyczne podłączanie się. 11. Praca zdalna - czym jest VPN i jak z niego korzystać. 12. Wprowadzenie do sieci komputerowych - niebezpieczeństwo sieci otwartych bezprzewodowych. 13. Niezabezpieczone protokoły sieciowe - HTTP FTP 14. Zaszyfrowana komunikacja w Internecie (Signal i WhatsApp) 15. Ochrona plików i dysków czyli podstawy szyfrowania. 16. Przedstawienie przykładów i nauka rozpoznawania niepożądanych maili i ich zawartości. 17. Odpowiednia weryfikacja odbiorcy i nadawcy. 18. Weryfikacją wiadomości e-mail 19. Weryfikacja i skan plików znajdujących się w załączniku. 20. Przykłady ataków oraz sposoby na ochronę przed nimi pod kątem zwykłego użytkownika 21. Phishing i td - Sposoby na zabezpieczenie się przed włamaniami i oszustwem w sieci 22. Programy antywirusowe i ich rola (omówienie popularnych programów i opis ich działania) 23. Tworzenie kopii zapasowych i ich odzyskiwanie po awarii. 24. Sposoby tworzenia backup’ów. 25. Podpis elektroniczny dokumentów w prosty i bezpieczny sposób. | [….] |
| **Wymagania dodatkowe** | W ramach realizacji szkolenia wymagane jest, aby:  - Szczegółowy harmonogram szkolenia został uzgodniony z Zamawiającym terminie minimum 14 dni przed terminem rozpoczęcia szkolenia  - Szkolenia zostaną przeprowadzone w maksymalnie 2 turach po 4 godziny  - Uczestnik szkolenia musi otrzymać pakiet materiałów szkoleniowych,  - Uczestnik po zakończeniu szkolenia musi otrzymać zaświadczenie ukończenia szkolenia - Uczestnik musi mieć możliwość bezpłatnego 14-sto dniowego kontaktu z trenerem po szkoleniu. | [….] |
| **Ilość** | Szkolenie dla 80 pracowników | [….] |

............................, dn. \_ \_ . \_ \_ . \_ \_ \_ \_r.

**KWALIFIKOWANY PODPIS ELEKTRONICZNY Wykonawcy**

**lub osób uprawnionych do składania oświadczeń**

**woli w imieniu Wykonawcy**