**Załącznik nr 1C do FORMULARZA OFERTOWEGO**

**Parametry techniczne i wyposażenie**

**CZĘŚĆ III – oprogramowanie do szyfrowania poczty wraz ze szkoleniem**

WYPEŁNIA WYKONAWCA:

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

Oferuję oprogramowanie do szyfrowania poczty wraz ze szkoleniem, następującego PRODUCENTA: ………………….…………………

MARKA/MODEL/TYP/OZNACZENIE HANDLOWE: ……………………………………………………………..

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 dostawy przedmiotu zamówienia wraz z jego rozpakowaniem, sprawdzeniem poprawności działania i ustawieniem w wyznaczonym przez Zamawiającego pomieszczeniu na terenie Urzędu.

Wykonawca zobowiązany do utylizacji na własny koszt wszelkich niepotrzebnych materiałów zabezpieczających urządzenia podczas transportu, w tym kartony, folie, taśmy klejące etc.

Wykonawca zobowiązany jest do ustalenia terminów dostaw z Zamawiającym, we wskazanym przez niego miejscu, z uwzględnieniem charakteru pracy Urzędu.

Potwierdzenie spełniania poniższych minimalnych warunków:

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Typ** | Oprogramowanie do szyfrowania poczty wraz ze szkoleniem | | **[….]** |
| **Wymagania techniczne** | W ramach dostawy Wykonawca zobowiązany jest do dostarczenia oprogramowania do szyfrowania wiadomości e-mail technologią “end to end” dla 100 użytkowników.  Dostarczone oprogramowanie musi zapewnić funkcjonalność minimalną:  - szyfrowanie algorytmem AES256 treści wiadomości,  - szyfrowanie algorytmem AES256 załączników,  - szyfrowanie algorytmem AES256 plików,  - szyfrowanie algorytmem AES256 katalogów,  - do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagany jest  dodatkowy płatny lub bezpłatny dostęp do usług internetowych, chmury, hostingu lub portalu  internetowego.  - do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagane jest  połączenie Internetowe.  - do odszyfrowania wiadomości nie jest potrzebne wysyłanie linków do oprogramowania  deszyfrującego.  - do odszyfrowania treści wiadomości nie jest wymagane instalowanie dodatkowego oprogramowania deszyfrującego.  - odszyfrowanie treści wiadomości, plików, katalogów, załączników email musi być możliwe na  popularnych systemach operacyjnych z środowiskiem graficznym: Windows XP, Windows Vista,  Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11, Ubuntu Desktop 20.04.3, Ubuntu  Desktop 21.10, Linux Mint 20.2, Fedora Workstation 35, macOS 11, Android od wersji 6.0  - szyfrowana zawartość wiadomości może zawierać nie tylko tekst,ale również elementy graficzne  takie jak: HTML, obrazki  - generowania bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla  szyfrowania,  - opieczętowania każdej wysłanej wiadomość sygnaturą, która jednoznacznie wskazuje na jej  oryginalność,  - zabezpieczenia każdego emaila dedykowanym unikalnym hasłem,  - posiadania wewnętrznej bazy haseł, która umożliwia:   1. export haseł do pliku, 2. import haseł z pliku 3. generowania ponownie haseł w bazie   - posiadania wewnętrznego raportu informującego administratora o szyfrowaniu email przy włączonej opcji generowania hasła dla każdej z nich,  - posiadania wewnętrznego raportu z historią szyfrowanych plików i katalogów wraz z przypisanym  hasłem szyfrującym,  - posiadania menu kontekstowego do szybkiego wybierania szyfrowania wiadomości emailowych,  plików i katalogów,  - pracy i pomocy zdalnej użytkownikom poprzez przejęcie zdalnego pulpitu również poza siecią  lokalną z użyciem jednorazowych wygenerowanych kodów autoryzacyjnych. Dodatkowo system  pracy zdalnej musi działać niezależnie od włączonej funkcji UAC w systemie Windows.  - integracji z komórką (Android, IOS, Windows Phone) umożliwiającą wygenerowanie sms-a z hasłem i docelowym kontaktem sms-owym,  - zabezpieczenia panelu ustawień oprogramowania poprzez hasło dostępowe,  - wykrywania fałszywych emaili - Antiphishing,  - wykrywania prób podszycia się pod dowolnego adresata - mechanizm ANTISPOOFING,  - wykrywania fałszywych linków i odsyłaczy w wiadomościach emailowych,  - wykrywanie niebezpiecznych dokumentów MS Office,  - wykrywanie niebezpiecznych rozszerzeń plików przesyłanych przez pocztę email,  - definiowania alarmów informujących o niebezpiecznych mailach i załącznikach,  - współpracę z serwerem producenta oprogramowania dostarczającym bazy reguł, sygnatur, zagrożeń phishingowych. Dostęp do tej bazy wymagany jest minimum na 4 lata. Baza reguł, sygnatur i zagrożeń phishingowych powinna posiadać min. 1 500 000 wpisów. Producent musi umożliwiać wyświetlanie ilości wpisów na aktualny dzień poprzez stronę Internetową. Wpisy do bazy muszą być weryfikowane min. 4 razy w ciągu dnia,  - alarmowanie o wybranych zagrożeniach phishingowych min. raz na miesiąc,  - współpracy z klientem Mozilla Thunderbird i Mozilla Thunderbird Portable dla systemów 32 i 64  Bit Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11. | | **[….]** |
| **Wymagania dodatkowe** | Oprogramowanie musi zostać dostarczone wraz z licencją wieczystą na użytkowanie oprogramowania z wsparciem technicznym i prawem do aktualizacji oprogramowania, bazami reguł, sygnatur i zagrożeń phishing przez minimum 48 miesięcy.  Oprogramowanie musi działać samodzielnie i do poprawnej jego pracy nie może wymagać innych licencji na oprogramowanie dodatkowe.  Oprogramowanie musi poprawnie działać z wykorzystywanym oprogramowaniem antywirusowym posiadanym przez Zamawiającego tj. ESET ENDPOINT ANTYVIRUS ważnego do dnia 25.04.2023  Oprogramowanie nie może wyłączać domyślnego antywirusa systemowego Windows.  Uwierzytelnienie użytkowników do systemu operacyjnego i kontrolera domeny musi odbywać się przy pomocy dedykowanego urządzenia sprzętowego. W ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest do dostarczenia 100 urządzeń autoryzacyjnych typu TOKEN, o wymaganiach minimalnych:  - Pamięć urządzenia sprzętowego musi umożliwiać zdefiniowania do 20 uwierzytelnień do systemu operacyjnego i kontrolera domenowego.  - Możliwość autoryzacji do systemu operacyjnego i kontrolera domeny musi być realizowana dedykowanym min. 6 znakowym PIN-em.  - Użytkownik zanim dokona logowania do systemu operacyjnego przy pomocy urządzenia sprzętowego musi mieć możliwość wyświetlenia zdefiniowanej przez administratora wewnętrzną PBI.  - Administrator Bezpieczeństwa Informacji musi mieć możliwość zarządzania treścią, która jest wyświetlana i akceptowana w procesie logowania do systemu operacyjnego i kontrolera domeny.  - Ważność certyfikatu bezpieczeństwa wystawianego przez producenta dla urządzeń autoryzujących typu TOKEN: minimum 48 miesięcy | **[….]** | |
| **Wdrożenie i szkolenie** | W ramach realizacji dostawy przedmiotu zamówienia, Wykonawca zobowiązany do przeprowadzenia wdrożenia rozwiązania na miejscu u Klienta, wraz z przeprowadzeniem szkolenie z zakresu użytkowania oprogramowania dla min. 2 administratorów, w zakresie min. 4 godzin. | | **[….]** |
| **Ilość** | 1 kpl. | | **[….]** |

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

**KWALIFIKOWANY PODPIS ELEKTRONICZNY Wykonawcy**

**lub osób uprawnionych do składania oświadczeń**

**woli w imieniu Wykonawcy**