Powiat Mławski
ul. Władysław Stanisława Reymonta 6
06-500 Mława

Załącznik Nr 2 do Regulaminu

**Or.272.9.2023**

# ISTOTNE WARUNKI UDZIELANIA ZAMÓWIENIA

w postępowaniu powyżej 30 000 zł netto, prowadzonym zgodnie z Regulaminem przy udzielaniu zamówień publicznych, których wartość nie przekracza kwoty, określonej w art. 2 ust. 1 pkt 1 ustawy z dnia 11 września 2019r. Prawo zamówień publicznych ( Dz. U. z 2023r., poz. 1605 ze zm.) (Zarządzenie Nr 10/2021 Starosty Mławskiego z dnia 20.01.2021r. ) w związku z realizacją przez Powiat Mławski projektu grantowego pn. „Cyfrowy Powiat", realizowanego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia – REACT-EU, Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia w zakresie:
- modułu nr 1: cyfryzacja: biur, jednostek publicznych, jednostek podległych i nadzorowanych Chmura obliczeniowa dla JST,
na:

**„Zakup oraz dostarczenie 3 sztuk urządzeń UTM na potrzeby Starostwa Powiatowego w Mławie "**

## I. Nazwa oraz adres zamawiającego

Zamawiający: **Powiat Mławski**
Reprezentowany przez **Zarząd Powiatu Mławskiego**

**Jerzego Rakowskiego – Starostę Mławskiego**
**Krystyna Zając – Wicestarosta**
Adres do korespondencji: **Władysława Stanisława Reymonta 6, 06-500 Mława**
**NIP: 569-17-60-040**
Godziny pracy: poniedziałek-piątek: 8:00-16:00
Tel. **23 655 29 00** Faks **23 655 26 22**

## II. Opis przedmiotu zamówienia

1. Specyfikacja głównych wymagań

**1)** Urządzenia UTM muszą spełniać wymagania opisane w niniejszym IWUZ.
**2)** Urządzenia muszą być fabrycznie nowe, wolne od wad fizycznych oraz prawnych, pełnowartościowe, nienoszące znamion użytkowania. Oferowany przedmiot zamówienia musi być w I gatunku, w pełni sprawny i funkcjonujący bez jakichkolwiek zakłóceń oraz zastrzeżeń. Wykonawca musi dostarczyć sprzęt w nienaruszonych fabrycznych oraz oryginalnych opakowaniach producenta.
**3)** Urządzenia muszą być zakupione w oficjalnym kanale sprzedaży producenta i posiadać pakiet usług gwarancyjnych, kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej.
**4)** Dostarczony przedmiot umowy musi być dopuszczony do obrotu i stosowania w

krajach UE. Musi posiadać odpowiednie i niezbędne certyfikaty, deklaracje i atesty zgodnie z obowiązującymi przepisami prawa oraz spełniać wszystkie warunki techniczne, użytkowe i jakościowe, określone przez Zamawiającego w opisie przedmiotu zamówienia.

**5)** Przedmiot zamówienia nie może pochodzić z żadnych pokazów ani wystaw, musi być pozbawiony praw i obciążeń osób trzecich, a także odpowiadający. Produkty elektryczne muszą spełniać wymogi niezbędne do oznaczenia produktów znakiem CE.

**6)** W przypadku, gdy w opisie przedmiotu zamówienia zostały wskazane znaki towarowe, patenty, normy, aprobaty, specyfikacje techniczne i systemy odniesienia lub pochodzenie materiałów, Zamawiający dopuszcza oferowanie materiałów równoważnych pod warunkiem, że zagwarantują one uzyskanie parametrów technicznych i eksploatacyjnych nie gorszych od założonych w dokumentacji. Równoważność polega na możliwości zaoferowania przedmiotu o takich samych lub lepszych parametrach technicznych.

**7)** Wszystkie oferowane komponenty wchodzące w skład urządzeń będą ze sobą kompatybilne i nie będą obniżać ich wydajności. Zamawiający nie dopuszcza sprzętu, w którym zaoferowane komponenty będą pracowały na niższych parametrach niż opisywane w IWUZ.

**Wymagania Ogólne**

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Powiat Mławski
ul. Władysław Stanisława Reymonta 6
06-500 Mława



**Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 10 portami Gigabit Ethernet RJ-45.
   - 2 gniazdami SFP 1 Gbps.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.

Powiat Mławski
ul. Władysław Stanisława Reymonta 6
06-500 Mława



**Funkcje Systemu Bezpieczeństwa:**

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy StatefulInspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - IntrusionPrevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Trafficshaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

**Polityki, Firewall**

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

**Połączenia VPN**

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/CounterMode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Wsparcie dla następujących typów uwierzytelniania: pre-sharedkey, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   - Możliwość monitorowania wybranego tunelu IPSecsite-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

- Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

**Routing i obsługa łączy WAN**

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equalcostmulti-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (BidirectionalForwardingDetection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

**Funkcje SD-WAN**

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

**Zarządzanie pasmem**

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

**Ochrona przed malware**

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.

4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

**Ochrona przed atakami**

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

**Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

**Kontrola WWW**

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja SafeSearch – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

**Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

**Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

**Logowanie**

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności

administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

**Certyfikaty**

Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

**Serwisy i licencje**

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

- kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandboxcloud, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

**Gwarancja oraz wsparcie**

Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

**Opisy do wymagań ogólnych**

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego

systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

2. Termin wykonania zamówienia - **21 dni kalendarzowych od podpisania umowy.**
3. Wykonawca jest związany ofertą 30 dni.
4. Bieg terminu związania rozpoczyna się wraz z upływem terminu składania ofert.

## III. Informacja o oświadczeniach i dokumentach, jakie mają dostarczyć Wykonawcy w celu potwierdzenia spełnienia warunków udziału w postępowaniu

1. Zamawiający wymaga, by każda oferta zawierała minimum następujące dokumenty:
   **1)** wypełniony i podpisany przez Wykonawcę formularz cenowo-ofertowy (wzór formularza stanowi **Załącznik nr 1 do niniejszych IWUZ**), **wraz z dokładną specyfikacją oferowanych urządzeń, w tym markę, model urządzenia.**
   **2)** aktualny odpis z właściwego rejestru albo aktualne zaświadczenia o wpisie do ewidencji działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub zgłoszenia do ewidencji działalności gospodarczej, wystawionego nie wcześniej niż 6 miesięcy przed upływem terminu składania oferty cenowej – oryginał lub kserokopia poświadczona przez Wykonawcę.
   **3)** Oświadczenie (wzór formularza stanowi **Załącznik nr 3 do IWUZ)**.
2. Dokument o którym mowa w ust. 1 pkt 2 może być dostarczony przed podpisaniem umowy.
3. Postępowanie prowadzone jest w języku polskim.

## IV. Informacja o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń i dokumentów

Wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy mogą przekazywać pisemnie, za pomocą faksu lub drogą elektroniczną.

## V. Osoby po stronie Zamawiającego uprawnione do porozumiewania się z Wykonawcami

1. Osobą uprawnioną do kontaktowania się z Wykonawcami i udzielania wyjaśnień dotyczących postępowania jest w sprawach proceduralnych jest Pan/Pani **Agnieszka Araszkiewicz**, (tel/faks, e-mail) **tel. 23 655 29 15, fax: 23 655 26 22 e-mail: agnieszka.araszkiewicz@powiatmlawski.pl,** zaś w sprawach

merytorycznych Pan Marcin Jurkiewicz (tel/faks, e-mail) **Marcin.Jurkiewicz@powiatmlawski.pl tel. 23 655 29 15, fax: 23 655 26 22.**

2. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie istotnych warunków udzielania zamówienia w godzinach pracy Zamawiającego od poniedziałku do piątku w godz. 8:00-16:00.

## VI. Miejsce i termin składania oraz otwarcie ofert

1. Ofertę cenową należy dostarczyć osobiście, wysłać pocztą do siedziby Zamawiającego pod adres, ul. Władysława Stanisława Reymonta 6, 06-500 Mława **w terminie do 12.09.2023r., do godz. 12:00. Ofertę należy składać w zamkniętych kopertach z opisem: „Zakup oraz dostarczenie 3 sztuk urządzeń UTM na potrzeby Starostwa Powiatowego w Mławie". Można także ofertę złożyć elektronicznie – drogą mailową– zaszyfrowany plik..** Hasło do pliku proszę przekazać w dniu otwarcia ofert. Decyduje data i godzina wpływu oferty do Zamawiającego**. Zamawiający dokona otwarcia ofert cenowych w dniu 12.09.2023r., o godz. 13:00 w swojej siedzibie** (adres jak wyżej).
2. Otwarcie ofert jest jawne.
3. Oferty niespełniające wymagań, określonych w IWUZ oraz nadesłane po wyznaczonym terminie zostaną odrzucone.
4. Bezpośrednio przed otwarciem ofert cenowych Zamawiający poda kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
5. Zamawiający zastrzega sobie prawo do unieważnienia prowadzonego postępowania, a Wykonawca ten fakt akceptuje i zobowiązuje się, że nie będzie wnosił żadnych roszczeń z tego tytułu wobec Zamawiającego.

## VII. Opis sposobu obliczania ceny

1. Na formularzu cenowo-ofertowym (**Załącznik Nr 1 do IWUZ**) należy przedstawić cenę netto i brutto przedmiotu zamówienia oraz stawkę VAT.
2. Wartość cenową należy wpisać w polskich złotych z precyzją do dwóch miejsc po przecinku oraz słownie.
3. Cena zawierać ma wszystkie koszty przedmiotu zamówienia.

## VIII. Kryteria oceny ofert

Zamawiający będzie się kierował następującymi kryteriami:

**- Cena – 100%**

I. Kryterium: Cena = $\frac{\text{Cena najtańszej oferty}}{\text{Cena oferty badanej}}$ x 100% (pkt)

- Zamawiający dokona oceny ofert przyznając punkty w ramach poszczególnych kryteriów oceny ofert, przyjmując zasadę, że 1% = 1 punkt.

## IX. Informacja dotycząca walut obcych w jakich mogą być prowadzone rozliczenia między zamawiającym i wykonawcą

Rozliczenia między Zamawiającym i Wykonawcą będą prowadzone w polskich złotych.

## X. Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. O wyborze oferty cenowej Zamawiający zawiadomi niezwłocznie Wykonawców, którzy ubiegali się o udzielenie zamówienia.
2. Zamawiający zawrze umowę niezwłocznie po przekazaniu zawiadomienia o wyborze oferty.
3. Jeżeli Wykonawca, którego oferta została wybrana, uchyli się od zawarcia umowy, Zamawiający wybierze ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzania ich ponownej oceny.
4. Zamawiający przekazuje projekt umowy (**Załącznik Nr 2 do IWUZ**), określającej warunki wykonania zamówienia. Zamawiający będzie żądał, aby umowa została zawarta i zrealizowana na warunkach określonych w tym projekcie.
5. Do prowadzonego postępowania nie przysługują Wykonawcom środki ochrony prawnej (protest, odwołanie, skarga) określone odpowiednio w przepisach ustawy Prawo zamówień publicznych.
6. Niniejsze postępowanie prowadzone jest na zasadach opartych na wewnętrznych uregulowaniach organizacyjnych bez zastosowania obowiązujących przepisów ustawy Prawo zamówień publicznych.

**Załączniki do IWUZ**

1. Formularz cenowo-ofertowy.
2. Projekt umowy.
3. Oświadczenie.

Signed by / Podpisano przez:
Jerzy Ryszard Rakowski
Date / Data: 2023-09-07 11:38

**ZATWIERDZAM**

**07.09.2023r.**

**Jerzy Rakowski**

.....
**(data i podpis Starosty Mławskiego)**