

### Zaproszenie do złożenia oferty cenowej

**Gmina Kozienice zaprasza do złożenia oferty na odnowienie systemu bezpieczeństwa składający się z dwóch urządzeń pracujących osobno nie w klastrze oraz oprogramowania.**

**Rodzaj zamówienia:** dostawa

Kod CPV – 48811000-6, 72611000-6

**Podstawa prawna** - art. 4 pkt.8 ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (tekst jedn. Dz.U. z 2019r. poz. 1843)

Postępowanie, którego wartość nie przekracza wyrażonej w złotych równowartości kwoty 30 000 euro, prowadzone w oparciu o Zarządzenie Nr 259/2016 Burmistrza Gminy Kozienice z dnia 01.12.2016r. w sprawie powołania komisji przetargowej i ustalenia regulaminu udzielania zamówień na dostawy, usługi i roboty budowlane oraz procedury obiegu dokumentów w zakresie udzielania zamówień publicznych w Urzędzie Miejskim w Kozienicach.

Postępowanie prowadzone w ramach procedury rozeznania rynku oraz w celu oszacowania wartości zamówienia, w tym kosztów jego realizacji.

#### **Zamawiający:**

Gmina Kozienice, ul. Parkowa 5, 26-900 Kozienice

NIP 812-18-28-216, REGON 670223333

tel. 048 611 71 00, faks 048 6142048, strona internetowa: [www.kozienice.pl](http://www.kozienice.pl)

adres poczty elektronicznej w postępowaniu: [piotr.kohut@kozienice.pl](mailto:piotr.kohut@kozienice.pl)

godziny urzędowania Zamawiającego:

- poniedziałek: 8:00 do 17:00
- wtorek-czwartek: 7:30 do 15:30
- piątek: 7:30 do 14:30

#### **I. Opis przedmiotu zamówienia**

1. **Przedmiotem zamówienia jest dostarczenie odnowienia systemu bezpieczeństwa składającego się z dwóch urządzeń pracujących w klastrze , oraz rozszerzenie o dodatkowe licencje .**
2. **Opis systemu o poniższej specyfikacji:**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

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

### **Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

### **Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum:
  - 20 portami Gigabit Ethernet RJ-45.
  - 2 gniazdami SFP 1 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

### **Parametry wydajnościowe:**

1. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 7.4 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 4.4 Gbps dla pakietów 64 B.
4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps.
5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 4 Gbps.
6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 500 Mbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps.
8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 190 Mbps.

### **Funkcje Systemu Bezpieczeństwa:**

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

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Analiza ruchu szyfrowanego protokołem SSL.
11. Analiza ruchu szyfrowanego protokołem SSH.

### **Polityki, Firewall**

System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW.

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać 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 musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

### Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
  - Wsparcie dla IKE v1 oraz v2.
  - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
  - Obsługa protokołu Diffie-Hellman grup 19 i 20.
  - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
  - 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.
  - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
  - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
  - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
  - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

### Routing i obsługa łącz WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
  - Routingu statycznego.
  - Policy Based Routingu.
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łącz WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

### Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

### Kontrola Antywirusowa

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

### Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Ochrona przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać 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) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

### Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

#### **Kontrola WWW**

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

#### **Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall musi umożliwiać 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. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

#### **Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

#### **Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.
- ICSA lub NSS Labs dla funkcji IPS.
- ICSA dla funkcji IPSec VPN.
- ICSA dla funkcji SSL VPN.

#### **Serwisy i licencje**

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

- a) 360 Protection (SD-WAN Orchestrator, SD-WAN Cloud Monitoring, FMG/FAZ Cloud, IPAM, IPS, AMP, App Ctrl, Web Filtering, AS, Security Rating, IoT Detection, Industrial Security, FortiConverter Svc, and ASE FortiCare)

W ramach postępowania wymagany jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi wersje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

#### **Interfejsy, Dysk:**

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 500

#### **Parametry wydajnościowe:**

1. System musi być w stanie przyjmować minimum 1GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

#### **Logowanie**

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
  - a. Listę najczęściej wykrywanych ataków.
  - b. Listę najbardziej aktywnych użytkowników.
  - c. Listę najczęściej wykorzystywanych aplikacji.
  - d. Listę najczęściej odwiedzanych stron www.
  - e. Listę krajów, do których nawiązywane są połączenia.
  - f. Listę najczęściej wykorzystywanych polityk Firewall.
  - g. Informacje o realizowanych połączeniach IPSec.
4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

#### **Raportowanie**

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

#### **Korelacja logów**

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
  - Malware.
  - Aplikacje sieciowe.
  - Email.
  - IPS.
  - Traffic.
  - Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

#### Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
  - a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
2. System musi umożliwiać zdefiniowanie co najmniej 3 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

#### Serwisy i licencje

1. System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
2. Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
3. FortiAnalyzer-VM Support FC1-10-LV0VM-149-02-DD Subscription license for the FortiGuard Indicator of Compromise (IOC) (for 1-6 GB/Day of Logs)

#### Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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.

#### Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. **Rozszerzone wsparcie serwisowe AHB/SOS**
2. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym /w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia przez okres 12 miesięcy.

**II. Termin wykonania zamówienia: do 14 dni.**

1. Wykonawca, w terminie do 14 dni od podpisania umowy dostarczy Zamawiającemu przedmiot zamówienia wraz z końcowym rozliczeniem.
2. W przypadku nie dotrzymania terminów, o których mowa powyżej Zamawiający zastrzega sobie prawo rozwiązania umowy z winy Wykonawcy naliczenie kar umownych.

**III. Wymagania w stosunku do Wykonawcy**

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:
  - 1.1. Posiadają wiedzę i doświadczenie niezbędną do wykonania niniejszego zamówienia.
  - 1.2. Posiadają odpowiedni potencjał techniczny oraz osoby zdolne do wykonania niniejszego zamówienia.
  - 1.3. Znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie niniejszego zamówienia.
  - 1.4. Nie podlegają wykluczeniu w okolicznościach, o których mowa w art. 24 ust. 1 pkt. 12-23 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych.
  - 1.5. Oświadczenie wykonawcy o spełnianiu warunków udziału w postępowaniu i barku podstaw do wykluczenia z postępowania (składane na druku oferty-zał. nr 1 do zaproszenia).

**IV. Przygotowanie oferty**

1. Ofertę należy sporządzić zgodnie z formularzem oferty stanowiącym załącznik nr 1 do niniejszego zaproszenia.
2. Oferta musi być sporządzona w formie pisemnej i być podpisana przez osobę uprawnioną.
3. W przypadku, gdy ofertę podpisuje osoba inna niż wynika to z dokumentów rejestrowych, do oferty należy dołączyć pełnomocnictwo, zgodne z wymaganiami Kodeksu cywilnego upoważniające do wykonania tej czynności.
4. Do oferty należy dołączyć dokumenty i oświadczenia, o których mowa w pkt. III. 3.
5. Wszystkie załączniki do oferty, stanowiące oświadczenia powinny być podpisane przez upoważnionego przedstawiciela. Zakres reprezentacji przedsiębiorcy musi wynikać z dokumentów przedstawionych przez Wykonawcę.
6. Kserokopie dokumentów muszą być poświadczane za zgodność z oryginałem przez Wykonawcę.
7. Koszty sporządzenia i złożenia oferty ponosi Wykonawca.
8. Wykonawca może złożyć w prowadzonym postępowaniu wyłącznie jedną ofertę obejmującą całość usług, o których mowa w pkt. 1.1. zaproszenia.

**V. Opis sposobu obliczenia ceny oferty**

1. Cenę oferty za wykonanie przedmiotu zamówienia Wykonawca wskaże w Formularzu oferty (zał. nr 1 do zaproszenia). Wykonawca zobowiązany jest do właściwego i szczegółowego wypełnienia druku oferty i załączników do oferty. Dane zawarte w ofercie są podstawą weryfikacji Wykonawcy.
2. Cena oferty ma być wyrażona w PLN jako cena brutto i winna obejmować wszystkie koszty i opłaty, jakie powstaną w związku z wykonaniem zamówienia, w tym w szczególności: materiały i czynności uznane przez Wykonawcę jako niezbędne do prawidłowego wykonania dostawy, opłaty niewymienione, które mogą wystąpić przy realizacji przedmiotu zamówienia, wszelkie podatki i opłaty, w tym należny podatek VAT, ewentualne opusty oraz inne składniki cenotwórcze.
3. Jeżeli ofertę złoży osoba fizyczna nieprowadząca działalności gospodarczej, w cenę oferty należy wliczyć składki na ubezpieczenie społeczne i zdrowotne oraz zaliczkę na podatek dochodowy, które to Zamawiający, zgodnie z obowiązującymi przepisami, zobowiązany byłby naliczyć i odprowadzić.
4. Cenę za wykonanie zamówienia należy wliczyć wg. kalkulacji własnej. W cenie ofertowej należy uwzględnić wszelkie koszty, jakie Wykonawca przewiduje ponieść na wykonanie dostawy.
5. Zamawiający wyklucza możliwość roszczeń Wykonawcy z tytułu błędnego skalkulowania ceny lub pominięcia elementów niezbędnych do wykonania zamówienia.

**VI. Miejsce i termin składania i otwarcia ofert**

1. Ofertę cenową sporządzoną na Formularzu oferty (zał. nr 1) wraz z załącznikami należy złożyć w siedzibie Urzędu Miejskiego w Kozenicach, ul. Parkowa 5, 26-900 Kozenice, w pok. Nr 111-Sekretariat, w terminie do dnia 26.10.2020 r. do godz. 12:00.

Ofertę cenową należy złożyć w zamkniętej kopercie opatrzonej napisem: „Oferta na odnowienie systemu bezpieczeństwa składający się z dwóch urządzeń pracujących osobno, nie w klastrze oraz oprogramowania.

2. " z dopiskiem „**Nie otwierać przed dniem 26.10.2020 r. przed godz. 12: 00**” Otwarcie ofert nie ma charakteru publicznego.
3. Oferty złożone po terminie wyznaczonym do składania ofert nie będą rozpatrywane. Oferty pozostaną u Zamawiającego bez otwierania.
4. Wykonawca może przed upływem terminu na składanie ofert zmienić lub wycofać swoją ofertę, składając pisemny wniosek do Zamawiającego.

**VII. Kryteria oceny ofert i ocena ofert**

1. Zamawiający dokona oceny ofert ważnych, spełniających wymagania określone w zaproszeniu, na podstawie kryterium:
  - 1.1. Cena-100%.
  2. Ocena ofert w kryterium „**Cena**” zostanie dokonana wg następujących zasad:  
Ocenie zostanie poddana cena brutto. Liczba punktów w kryterium „cena” (C) zostanie obliczona na podstawie poniższego wzoru:

$$C = \frac{C_{min}}{C_o} \times 100\%$$

gdzie:

C	liczba punktów za kryterium „cena”
C <sub>min</sub>	najniższa cena oferty brutto z ocenianych ofert (zł)
C <sub>o</sub>	cena oferty brutto określona w badanej ofercie (zł)

2. Najwyższa liczba punktów wyznaczy najkorzystniejszą ofertę.

**VIII. Inne postanowienia**

1. W toku rozpatrywania ofert cenowych Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonej oferty cenowej oraz prowadzić dodatkowe negocjacje z Wykonawcami, którzy odpowiedzieli na zapytanie ofertowe.
2. Zamawiający drogą elektroniczną powiadomi o wyborze Wykonawcę, którego oferta cenowa zostanie wybrana.
3. Zamawiający może unieważnić postępowanie bez podania przyczyny. Z tego tytułu, w stosunku do Zamawiającego, nie będą przysługiwać Wykonawcy żadne roszczenia.
4. Forma udzielenia zamówienia - umowa.
5. Istotne postanowienia i warunki, które zostaną wprowadzone do treści umowy zawiera projekt umowy - zał. nr 2 do niniejszego zaproszenia. Zamawiający zawrze umowę z wybranym Wykonawcą wg wzoru zawartego w załączniku nr 2.
6. Wymagany okres gwarancji na przedmiot umowy wynosi min. 60 miesięcy i będzie liczony od daty odbioru przedmiotu zamówienia.
7. Pytania do postępowania można zadawać drogą elektroniczną lub pisemną w terminie do dnia 23.10.2020 r. do godz. 14:00 /liczy się data i godz. wpływu do Zamawiającego/. Zamawiający udzieli odpowiedzi na pytania pocztą elektroniczną w dniu następnym.
8. Na zapytania złożone po dniu 23.10.2020 r. Zamawiający nie będzie udzielał odpowiedzi.
9. **Zamawiający informuje, że odmowa podpisania umowy przez Wykonawcę, którego oferta została wybrana w niniejszym postępowaniu, z jego winy, może skutkować, że w kolejnych postępowaniach oferta takiego Wykonawcy nie będzie rozpatrywana (będzie podlegać odrzuceniu).**

**IX. Informacja dotycząca ochrony danych osobowych**

Zgodnie z art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) - dalej RODO Gmina Kozienice informuje, iż:

1. Administratorem Pani/Pana danych osobowych : Burmistrz Gminy Kozienice
2. Siedziba Administratora: Urząd Miejski, ul. Parkowa 5, 26-900 Kozienice
3. Kontakt z Inspektorem Ochrony Danych- [iod@kozienice.pl](mailto:iod@kozienice.pl)



4. Pani/Pana dane osobowe przetwarzane będą w celu realizacji zamówienia - na podstawie Art. 6 ust. 1 lit. b i c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego oraz w celu archiwizacji.
5. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty uczestniczące w realizacji umowy oraz wszyscy którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29 stycznia 2004r. - Prawo zamówień publicznych (tj. Dz. U. z 2018r. poz. 1986) a także podmioty przetwarzające dane na podstawie zawartych umów.
6. Pani/Pana dane osobowe przechowywane będą przez okres obowiązywania umowy, a następnie 10 lat po zakończeniu okresu obowiązywania umowy. Okres ten dotyczy również Wykonawców, którzy złożyli oferty i nie zostały one uznane jako najkorzystniejsze (nie zawarto z tymi Wykonawcami umowy/zlecenia).
7. obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
8. Posiada Pani/Pan prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania.
9. Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego .
10. Podanie danych osobowych jest dobrowolne, jednakże odmowa podania danych może skutkować odmową zawarcia umowy.
11. nie przysługuje Pani/Panu:
  - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
    - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
  - na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

**Załączniki:**

1. Formularz oferty - zał. nr 1.
2. Wzór umowy-zał. nr 2.

**Sprawę prowadzi:**

- Pan/Pani Piotr Kohut. e-mail: piotr.kohut@kozienice.pl

Wydział Kadr, obsługi Rady i Informatyzacji Urzędu Miejskiego w Kozienicach  
tel. 48 6117193

BURMISTRZ GMINY KOZIENICE

mgr Piotr Kozłowski



ADWOKAT  
Andrzej Kowalik



Załącznik nr 1 – Wzór Formularza Oferty

<b>Pieczęć Wykonawcy/wców</b>	..... <b>Miejscowość i data</b>
-------------------------------	------------------------------------

Nr tel/fax .....

e-mail: .....

Województwo:.....

Adres do korespondencji: .....

.....

NIP .....Regon.....KRS/CEiDG.....  
(podać wszystkie dane)

**GMINA KOZIENICE**  
ul. Parkowa 5  
26-900 Kozienice

<b>OFERTA CENOWA</b>
----------------------

**W odpowiedzi na zaproszenie do złożenia oferty na odnowienie systemu bezpieczeństwa składający się z dwóch urządzeń pracujących osobno, nie w klastrze oraz oprogramowania.”**

**Ja/My niżej Podpisany/podpisani**

.....

(dane osoby upoważnionej do podpisania oferty)

działając w imieniu i na rzecz Wykonawcy/wykonawców<sup>1</sup>:

Lp.	Nazwa (y) Wykonawcy (ów)	Adres (y) Wykonawcy (ów)

uwzględniając zakres, warunki i wymagania zawarte w zaproszeniu, składamy niniejszą ofertę:

1. Oferujemy wykonanie zamówienia w zakresie określonym w zaproszeniu, zgodnie z opisem przedmiotu zamówienia :

**za cenę brutto** ..... **PLN, słownie:** .....

.....

2. Zamówienie wykonamy w terminie: **14 dni** od dnia podpisania umowy.

<sup>1</sup> Podać nazwę Wykonawcy, a w przypadku wykonawców występujących wspólnie należy podać nazwy i adresy wszystkich wykonawców (wszystkich wspólników spółki cywilnej lub członków konsorcjum)

3. Oświadczamy, że na wykonaną dostawę udzielamy **60 miesięcznej gwarancji jakości i rękojmi**, liczonej od daty końcowego odbioru przedmiotu niniejszego postępowania.

4. Oświadczamy, że:

- 1) Powyższa cena uwzględnia wszystkie koszty, jakie ponosi zamawiający w przypadku wyboru niniejszej oferty,
- 2) Zapoznaliśmy się z otrzymanymi dokumentami, w pełni je akceptujemy i nie wnosimy do nich zastrzeżeń oraz przyjmujemy warunki w nich zawarte,
- 3) Spełniamy warunki udziału w postępowaniu o których mowa w pkt. III.1 zaproszenia do złożenia oferty, tj.:
  - posiadamy wiedzę i doświadczenie niezbędne do wykonania niniejszego zamówienia,
  - dysponujemy osobami posiadającymi odpowiednie uprawnienia zawodowe do wykonania zamówienia,
  - znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie niniejszego zamówienia,
- 4) Nie podlegamy wykluczeniu z postępowania w okolicznościach, o których mowa w art. 24 ust. 1 pkt 12-23 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych.
- 5) Wobec mnie/mojej Firmy nie toczy się żadne postępowanie likwidacyjne lub upadłościowe i nie figuruję/żadna z osób reprezentujących moją Firmę nie figuruje w Krajowym Rejestrze Karnym,
- 6) Zamówienie wykonamy siłami własnymi/ przy pomocy następujących podwykonawców \*  
(\*niewłaściwe skreślić) .....

.....  
którym powierzymy wykonanie następujących części zamówienia .....

5. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO<sup>1)</sup> wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu. (W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO - *treść oświadczenia wykonawcy nie dotyczy*).

6. W przypadku przyznania nam zamówienia zobowiązujemy się do zawarcia umowy na warunkach zawartych w projekcie umowy, w miejscu i terminie wyznaczonym przez Zamawiającego.

7. Oświadczam, że pozostaje związany ofertą na okres 30 dni, licząc od dnia wyznaczonego do złożenia oferty.

8. Załącznikami do niniejszej oferty są:

1) .....

2) .....

3).....

4) .....

5).....

(podpis osoby/osób uprawnionych do reprezentowania  
Wykonawcy/Wykonawców)

## UMOWA

zawarta w Kozienicach  
dnia .10.2020

pomiędzy:

Gminą Kozienice z siedzibą w Kozienicach (26-900), ul. Parkowa 5 NIP: 8121828216, REGON: 670223333 zwaną dalej **Zamawiającym**, reprezentowaną przez:  
- Pana Piotra Kozłowskiego - Burmistrza Gminy Kozienice przy kontrasygnacie Pani Moniki Makulec Soboty -  
Skarbnika Gminy Kozienice

a:

.....  
NIP: ....., REGON: .....  
zwaną dalej **Wykonawcą**, reprezentowaną przez:

o następującej treści:

### PRZEDMIOT UMOWY

#### § 1

**Przedmiotem umowy jest odnowienie systemu bezpieczeństwa składający się z dwóch urządzeń pracujących osobno nie w klastrze oraz oprogramowania**

### WYNAGRODZENIE

#### § 2

1. Za wykonanie przedmiotu umowy określonego w § 1 **Zamawiający** zobowiązuje się zapłacić **Wykonawcy** wynagrodzenie w łącznej wysokości ..... zł **brutto** (słownie: .....złotych 00/100 groszy).
2. Wynagrodzenie, o którym mowa w ust.1 jest stałe i obejmuje całość wynagrodzenia należnego **Wykonawcy** z tytułu niniejszej umowy, nie może ulegać zmianom w trakcie realizacji umowy oraz obejmuje wszelkie koszty i wydatki **Wykonawcy** związane z realizacją przedmiotu umowy, z uwzględnieniem podatku od towarów i usług, innych opłat oraz ewentualnych upustów i rabatów.
3. Wynagrodzenie zostanie wypłacone przelewem na rachunek bankowy wskazany na prawidłowo wystawionej fakturze/rachunku VAT, dostarczonego do siedziby **Zamawiającego**.
4. Wynagrodzenie będzie płatne w terminie 14 dni od dnia wpłynięcia na sekretariat Urzędu Miejskiego w Kozienicach (siedziby **Zamawiającego**) prawidłowo wystawionej faktury/rachunku VAT po podpisaniu przez obie strony umowy bezusterkowego protokołu odbioru przedmiotu umowy stanowiącego *Załącznik Nr 2* do niniejszej umowy (dostarcza wykonawca).

### KARY UMOWNE

#### § 3

1. W przypadku nie dostarczenia przedmiotu umowy w terminie określonym w zapytaniu ofertowym (sygn. akt. KI.132.20.2020 z dnia 20 października 2020 r.) stanowiącym *Załącznik Nr 1* do niniejszej umowy **Wykonawca** zapłaci karę umowną w wysokości 1% całkowitej wartości wynagrodzenia brutto określonego w § 2 ust. 1 niniejszej umowy za każdy dzień opóźnienia.
2. W przypadku odstąpienia przez **Zamawiającego** od umowy z przyczyn zależnych od **Wykonawcy**, **Wykonawca** zapłaci karę umowną w wysokości - 30% wartości wynagrodzenia całkowitego brutto za wykonanie przedmiotu umowy, określonego w § 2 ust. 1 niniejszej umowy.
3. **Zamawiający** zastrzega sobie prawo potrącania kar umownych z bieżącego wynagrodzenia **Wykonawcy** i na co **Wykonawca** wyrazi zgodę.

4. **Zamawiający** ma prawo dochodzić odszkodowania przewyższającego wysokość kary umownej - na zasadach Kodeksu Cywilnego - do wysokości rzeczywiście poniesionej szkody.

W przypadku opóźnienia w zapłacie wynagrodzenia wynikającego z treści niniejszej umowy **Zamawiający** zobowiązuje się do zapłaty **Wykonawcy** odsetek ustawowych za opóźnienie.

#### §4

1. W ramach świadczonej usługi Usługodawca zobowiązuje się do świadczenia usług serwisowych i opieki autorskiej przez okres 12 miesięcy, w zakresie:
  - a) Zapewnienie stałego rozwoju oprogramowania oraz dostosowywania do obowiązującego stanu prawnego.
  - b) Otrzymywanie bezpłatnych aktualizacji systemu.
  - c) Pomoc telefoniczna i mailowa dla użytkowników systemu w dni robocze w godzinach 8.00 - 16.00.
2. W przypadku przedłużenia umowy na kolejny okres, postanowienia ust. 1 mają zastosowanie do nowego okresu obowiązywania umowy.

### POSTANOWIENIA KOŃCOWE

#### § 5

1. Umowa wiąże strony z dniem jej podpisania przez **Wykonawcę** i **Zamawiającego** i zostaje zawarta na czas spełnienia wszystkich świadczeń w niej zawartych.
2. **Wykonawca** zobowiązany jest do odesłania podpisanej umowy w dniu podpisania na adres mailowy [urząd@kozienice.pl](mailto:urząd@kozienice.pl) oraz na adres korespondencyjny **Zamawiającego** (Urząd Miejski w Kozienicach, ul. Parkowa 5, 26-900 Kozienice).
3. W sprawach nieuregulowanych umową stosuje się przepisy Kodeksu Cywilnego i Ustawy o prawie autorskim i prawach pokrewnych.
4. **Wykonawca** i **Zamawiający** oświadczają, że dołożą wszelkich starań, aby ewentualne spory, jakie mogą powstać przy realizacji postanowień niniejszej umowy były rozwiązywane polubownie poprzez bezpośrednie negocjacje.
5. Ewentualne spory, które mogą zaistnieć między stronami na tle wykonywania niniejszej umowy, których nie uda się rozwiązać polubownie w bezpośrednich negocjacjach, będą rozstrzygane przez sąd wg właściwości miejscowej **Zamawiającego**.
6. Zmiany i uzupełnienia umowy wymagają formy pisemnej pod rygorem nieważności.
7. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, jeden dla **Wykonawcy**, jeden dla **Zamawiającego**.

**WYKONAWCA**

**ZAMAWIAJĄCY**