Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską

Księżpol, 17.10.2024 r.

BGK.271.2.82.2024.AK

ZAPYTANIE WYCENY CENOWEJ

Niniejsze zapytanie nie stanowi zaproszenia do składania ofert w rozumieniu przepisów ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz.U. z 2024 r. poz. 1061 ze zm.) i podstawy do udzielenia zamówienia w rozumieniu przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz.U. z 2024 r. poz. 1320 ze zm.).

Zgodnie z Rozdziałem 5 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz.U. z 2024 r. poz. 1320 ze zm.) Zamawiający przed wszczęciem postępowania zobowiązany jest do ustalenia wartości zamówienia.

W celu ustalenia wartości zamówienia, Zamawiający zaprasza potencjalnych Wykonawców do zapoznania się z załączoną informacją o wymaganiach dotyczących przedmiotu zamówienia i złożenia informacji dotyczącej szacunkowej wartości zamówienia.

Gmina Księżpol z siedzibą w Księżpolu, ul. Biłgorajska 12, NIP: 918-19-95-823 w ramach realizacji projektu pn. „Wdrożenie infrastruktury ochrony danych w Gminie Księżpol" realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, w ramach Projektu grantowego „Cyberbezpieczny samorząd" zwraca się z prośbą o wstępne oszacowanie wartości zamówienia, zgodnie z poniższym opisem

I. PRZEDMIOT ZAMÓWIENIA:

Zakup infrastruktury sieciowej wraz z wyposażeniem w ramach projektu „Cyberbezpieczny Samorząd" Nr FERC.02.02-CS.01-001/23 „Wdrożenie infrastruktury ochrony danych w Gminie Księżpol"

II. OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA:

Przedmiotem zamówienia jest dostawa sprzętu informatycznego oraz serwisów zgodnie z poniższym zestawieniem:

1. Przełącznik agregacyjny – 3 szt
2. Przełącznik dostępowy – 3 szt
3. Zasilacz UPS z dodatkową baterią – 1 szt
4. Serwis audyt podatności i NBD dla UTM
5. Dyski SSD SAS do macierzy dyskowej – 6 szt

III. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przełącznik agregacyjny -3 szt

- **Porty przełącznika**: minimum 24x 1/10GBase-X SFP+ oraz minimum 2x 40GBase-X QSFP
- **Port konsolowy:** RJ45 (RS-232)
- **Port zarządzania:** RJ45 (10/100/1000Base-T RJ45)
- **Port USB:** minimum 1 port
- **Szybkość przełączania:** minimum 640Gb/s
- **Przepustowość:** minimum 476Mp/s (dla pakietów 64Kb)
- **Bufor pakietów:** minimum 1,5MB
- **Ramki Jumbo:** minimum 12k
- **Tablica adresów MAC:** minimum 32k
- **Adresy MAC – Multicast:** minimum 4k
- **Tablica ACL:** minimum 2,7k wej. oraz 1k wyj.
- **Tablica VLAN:** minimum 4094
- **Taktowanie procesora:** minimum 1,25GHz
- **Pamięć Flash:** minimum 128MB
- **Pamięć RAM:** minimum 512MB
- **Temperatura pracy:** zakres minimum 0°C - 50°C
- **Zasilanie:** zabudowany zasilacz 230V AC + redundantne zasilanie 48V DC
- **Pobór mocy:** maksymalnie 70W
- **Zabezpieczenie przeciwprzepięciowe:** minimum 6kV
- **Wymiary:** maksymalna: szerokość 440 mm, wysokość 44mm , głębokość 318mm
- **Obudowa:** metalowa z aktywnym chłodzeniem przeznaczona do montażu w szafie rack 19" (mocowania w komplecie)
- **Certyfikaty bezpieczeństwa**: CE, RoHS
- **Algorytm pracy:** Store and Forward
- **Obsługa VLAN:** Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ
- **DHCP:** IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server
- **Drzewo rozpinające:** IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding, Loopback Detection, Fast Link
  Protekcja ringowa: ITU-T G.8032 – recovery time < 50ms
- **Agregacja linków:** IEEE 802.3ad (LACP), 128 groups per device / 8 ports per group, load balance
- **Bezpieczeństwo:** Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,
- **Multicast:** IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM,
- **QoS:** 8 kolejek na port, Bandwidth Control, Flow Control: HOL, IEEE802.3x, Flow Redirect, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, PRI Mark/Remark, IEEE 802.1p, Metody kolejkowania: Strict Priority, Weighted Deficit Round Robin, Strict priority in Weighted Deficit Round Robin;
- **Lista Kontroli Dostępu:** IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Accouting based ACL,

Statistics based on ACL, Standard and Expanded ACL based on IP Protocol and IP Precedence, Vlan Tag/Untag, Możliwość konfiguracji reguł dla portów oraz VLAN

- **Diagnostyka:** sFlow, Traffic Analysis, RSPAN, Ping, Trace Route, Dying GASP, DDM
- **Zarządzanie:** TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), DNS Client, SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, CPU Mirror, IEEE 802.3ah/802.1ag OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (min. 4 urządzenia w jednym stosie) - sprzętowe łączenie w stosy
- **Oprogramowanie oraz wsparcie techniczne:** oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług
- **Gwarancja:** limited lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat.
- **Akcesoria:** (dla każdego przełącznika)
  a) Dodatkowy redundantny zasilacz DC
  b) 2 szt modułów optycznych QSFP+ o specyfikacji:
    - Typ interfejsu: QSFP+
    - Typ modułu: Duplex
    - Medium transmisyjne: SingleMode
    - Typ transmisji: Duplex
    - Typ złącza: LC/UPC
    - Przepływność: 40 Gb
    - Długość fali TX: 1310 nm
    - Sposób transmisji: CWDM [1270, 1290, 1310, 1330 nm]
    - Rodzaj modulacji: NRZ
    - Nadajnik: DFB/DML
    - Odbiornik: PIN
    - Dystans: 10 km
    - Temperatura pracy: 0|70 °C
  c) 2 szt modułów optycznych SFP+ o specyfikacji:
    - Typ interfejsu: SFP+
    - Typ modułu: Duplex
    - Medium transmisyjne: SingleMode
    - Typ transmisji: Duplex
    - Typ złącza: LC/UPC
    - Przepływność: 10 Gb
    - Długość fali TX: 1310 nm
    - Sposób transmisji: 1310 nm
    - Rodzaj modulacji: NRZ
    - Nadajnik: DFB
    - Odbiornik: PIN
    - Dystans: 10 km
    - Temperatura pracy: -5|70 °C

2. Przełącznik dostępowy – 3 szt

- **Porty przełącznika**: minimum 48x 10/100/1000Base-T z obsługa PoE oraz minimum 4 porty 10GE SFP+; Porty SFP+ 10GE obsługujące moduły 1GE SFP;
- **Stackowanie:** możliwość połączenia minimum 4 przełączników w stos za pomocą portów SFP+ bez dedykowanego okablowania
- **Port konsolowy:** RJ45 (RS-232)
- **Port zarządzania:** RJ45 (10/100Base-T RJ45)
- **Port USB:** minimum 1 port co najmniej w standardzie 2.0
- **Szybkość przełączania**: minimum 176 Gb/s
- **Przepustowość**: minimum 130 Mp/s (dla pakietów 64Kb)
- **Bufor pakietów:** minimum 1,5MB
- **Ramki Jumbo:** minimum 10k
- **Tablica adresów MAC:** minimum 16k
- **Adresy MAC – Multicast:** minimum 1k
- **Tablica ACL:** minimum 384
- **Tablica VLAN:** minimum 4094
- **Tablica routingu:** minimum 512 dla IPv4, w tym IPv6. Dopuszcza się rozwiązania współdzielące tablicę routingu dla IPv4 oraz IPv6 w maksymalnej proporcji 4:1.
- **Tablica ARP:** minimum 512
- **Taktowanie procesora:** minimum 800MHz
- **Pamięć Flash:** minimum 128MB
- **Pamięć RAM:** minimum 256MB
- **Obsługa PoE:** minimum IEEE 802.3 af/at
- **Budżet mocy PoE:** minimum 740W
- **Temperatura pracy:** zakres minimum 0°C - 50°C
- **Wilgotność względna:** zakres minimum 10% - 90% (bez kondensacji)
- **Zasilanie:** zabudowany zasilacz - 230V AC
- **Redundantne zasilanie:** zabudowany zasilacz – 52-57V DC
- **Pobór mocy:** maksymalnie 900W
- **Zabezpieczenie przeciwprzepięciowe:** minimum 4kV
- **Wymiary:** maksymalna: szerokość 440 mm, wysokość 44mm , głębokość 320mm
- **Obudowa:** metalowa z aktywnym chłodzeniem przeznaczona do montażu w szafie rack 19" (mocowania w komplecie)
- **Certyfikaty bezpieczeństwa**: CE, RoHS
-
- **Algorytm pracy:** Store and Forward
- **Obsługa VLAN:** Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ
- **DHCP:** IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server
- **Protokoły drzewa rozpinającego:** IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding,
- **Protekcja ringowa:** ITU-T G.8032 – recovery time < 50ms, Loopback Detection, Fast Link
- **Protokoły routingu:** Static Routing, RIPv1/v2, RIPng, OSPFv2/v3, BGP4, BGP4+, OSPF multiple process, LPM Routing, Policy-based Routing (PBR) IPv4/IPv6, VRRP, IPv6 VRRPv3, URPF IPv4/IPv6, ECMP, BFD, Static Multicast Route, Multicast Receive Control, Illegal Multicast Source Detect

- **Agregacja linków:** IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group, load balance
- **Bezpieczeństwo:** Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,
- **Multicast:** IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication
- **QoS:** 8 kolejek na port, Bandwidth Control, Flow Control: HOL, IEEE802.3x, Flow Redirect, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, PRI Mark/Remark, IEEE 802.1p, Metody kolejkowania: Strict Priority, Weighted Deficit Round Robin, Strict priority in Weighted Deficit Round Robin;
- **Lista Kontroli Dostępu:** IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Vlan Tag/Untag, Możliwość konfiguracji reguł dla portów oraz VLAN
- **Diagnostyka:** sFlow, Traffic Analysis, VCT, Ping, Trace Route,
- **Zarządzanie:** TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), DNS Client, SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (min. 4 urządzenia w jednym stosie) - sprzętowe łączenie w stosy
- **Oprogramowanie oraz wsparcie techniczne:** oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług
- **Gwarancja:** lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat.
- **Akcesoria:** (dla każdego przełącznika)

  d) 4 szt modułów optycznych SFP+ o specyfikacji:
    - Typ interfejsu: SFP+
    - Typ modułu: Duplex
    - Medium transmisyjne: SingleMode
    - Typ transmisji: Duplex
    - Typ złącza: LC/UPC
    - Przepływność: 10 Gb
    - Długość fali TX: 1310 nm
    - Sposób transmisji: 1310 nm
    - Rodzaj modulacji: NRZ
    - Nadajnik: DFB
    - Odbiornik: PIN
    - Dystans: 10 km
    - Temperatura pracy: -5|70 °C

3. Zasilacz UPS z dodatkową baterią – 1 szt

PARAMETR	CECHA/WARTOŚĆ/WŁAŚCIWOŚĆ
Minimalne wymagania techniczne dla jednostki UPS	Moc znamionowa jednostki nie mniej niż 1980W/ 2200VA Montowany w szafie RACK (komplet uchwytów w zestawie) Technologia Podwójnej konwersji (online) Temperatura eksploatacji 0 - 40 °C • Wilgotność względna podczas pracy 0 - 95 % • Hałas słyszalny w odległości 1 m od powierzchni urządzenia max 55 dBA • Rozpraszanie ciepła w trybie online 535,00 BTU/h • Sprawność: Praca on-line ≥ 92% przy pełnym obciążeniu • Klasa ochrony IP 20 • Klasa energetyczna sprzętu przeciwprzepięciowego 340J • automatyczne włączenie UPS-a po powrocie zasilania • możliwość zimnego startu • tryb ECO
Parametry wejściowe	• Nominalne napięcie wejściowe 230V • Częstotliwość wejściowa 40–70 Hz (wykrywanie automatyczne) • Typ gniazda wejściowego: IEC-320 C20 • Zmienny zakres napięcia wejściowego: pełne obciążenie 160 – 275V, połowa obciążenia 100-275V
Parametry wyjściowe	• Napięcie wyjściowe 220, 230, 240V • Częstotliwość na wyjściu zsynchronizowana z siecią zasilającą 50/60 Hz (±3Hz dla zasilania z sieci lub ±0.1Hz dla zasilania z baterii) • Współczynnik szczytu 3: 1 • Typ przebiegu sinusoida • Złącza/gniazda wyjściowe (8) IEC 320 C13, (2) IEC 320 C19 • Układ obejściowy (bypass) wewnętrzny tor obejściowy (automatyczny lub ręczny)
Akumulatory i czas podtrzymania	• Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny • Czas autonomii: 20 minuty 11 sekundy dla pełnego obciążenia 45 minut dla połowy obciążenia • Typowy czas ładowania 3 godziny • Oczekiwana żywotność akumulatora (lata) 3 – 5 • Możliwość rozszerzenia czasu podtrzymania poprzez dodanie do 10 zewnętrznych pakietów akumulatorowych • Baterie wymieniane na gorąco • Automatyczny test akumulatora
Komunikacja i zarządzanie	• Gniazdo do montażu karty WEB/SNMP- Smart Slot x1 (Zasilacz dostarczany wraz z kartą zarządzania sieciowego oraz czujnikiem temperatury) • Porty komunikacyjne: RJ-45, Smart-Slot, USB • Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD • Alarm dźwiękowy: Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia • Awaryjny wyłącznik zasilania (EPO)
Certyfikaty, zgodności oraz gwarancja	• CE, EAC, REACh, RoHS • 3 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulatory

Oprogramowanie	• Dostępne oprogramowanie do zarządzania/monitorigu dla VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®.
Dodatkowy moduł bateryjny	• Moduł bateryjny kompatybilny z oferowanym UPS, tego samego producenta, montowany w szafie RACK (komplet uchwytów w zestawie)

4. Serwis audyt podatności i NBD dla UTM

Zamawiający posiada urządzenie UTM Stormshield SN220, w ramach podniesienia poziomu bezpieczeństwa zamawiający oczekuje dostawy dodatkowych modułów:

1. Serwis Audyt Podatności ważny do 30.06.2026 r.
2. Serwis Next Business Day ważny do 30.06.2026 r.

Wykonawca może zaoferować rozwiązanie równoważne o minimalnych wymaganiach opisanych poniżej:

- Warunki równoważności:

Zamawiający uzna, że zaoferowane rozwiązanie posiada równoważne cechy z przedmiotem zamówienia, jeżeli będzie ono zawierało funkcjonalności co najmniej tożsame lub lepsze od określonych w poniższym opisie przedmiotu zamówienia w zakresie posiadanej funkcjonalności. W przypadku zaproponowania wersji równoważnej Wykonawca zobowiązany jest załączyć do oferty opis i dane techniczne zaproponowanego rozwiązania umożliwiające porównanie go z wszystkimi parametrami wymaganymi niniejszym opisem przedmiotu zamówienia w tym zgodność posiadanego oprogramowania z zaproponowanym rozwiązaniem. Dodatkowo Zamawiający zastrzega sobie prawo do zweryfikowania funkcjonalności, wydajności i kompatybilności zaoferowanego rozwiązania równoważnego poprzez analizę jego możliwości. W przypadku skorzystania przez Zamawiającego z ww. uprawnienia wykonawca jest zobowiązany w terminie 5 dni od dnia otrzymania od Zamawiającego wezwania do dostarczenia testowej wersji zaproponowanego rozwiązania dostarczyć to rozwiązanie do siedziby Zamawiającego. W przypadku zaproponowania wersji równoważnej Wykonawca zobowiązany jest dodatkowo przeprowadzić w cenie oferty pełen proces migracji Systemu Zamawiającego. Migracja dotyczyć musi całego oprogramowania wchodzącego w skład Systemu. Podczas procesu migracji w nowym systemie muszą zostać odwzorowane wszystkie zadania aktualnie zdefiniowane w systemie. Proces migracji Systemu nie może w żaden sposób wpływać na działanie środowiska, w szczególności proces migracji nie może wymuszać konieczności czasowego przestoju Urzędu, a migracja musi odbyć się poza godzinami jego pracy. Proces migracji nie może generować dla Zamawiającego żadnych dodatkowych kosztów w tym związanych z zakupem dodatkowego oprogramowania, licencji czy urządzeń. W przypadku dostawy rozwiązania równoważnego zamawiający wymaga przeprowadzenia certyfikowanego przez producenta szkolenia dla administratora Urzędu – co najmniej 3 dni po 8 godzin, zakończone egzaminem producenta.

OBSŁUGA SIECI

- Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (Firewall)

- Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
- Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
- Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
    - Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
    - Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
    - Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
    - Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
    - Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
    - Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
    - Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
    - System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

INTRUSION PREVENTION SYSTEM (IPS)

- System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
- Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
- Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
- Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
- Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.

- Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
- Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
- Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
- Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
- Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
- Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. Moduł musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci.
- Powyższy moduł ma nie tylko wykrywać oprogramowanie ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

- Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
- Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
- Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
- Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

- Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
- Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
- Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
- Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

OCHRONA ANTYSPAM

- Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
- Ochrona antyspam ma działać w oparciu o:
  a. białe/czarne listy,
  b. DNS RBL,
  c. Skaner heurystyczny.

- W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
- Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

- Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
- Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
  a. PPTP VPN,
  b. IPSec VPN,
  c. SSL VPN.
- SSL VPN ma działać co najmniej w trybach tunelu i portalu.
- Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
- Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
- Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
- Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
- Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

- Urządzenie ma posiadać wbudowany filtr URL.
- Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
- Administrator ma mieć możliwość dodawania własnych kategorii URL.
- Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
  a. blokowanie dostępu do adresu URL,
  b. zezwolenie na dostęp do adresu URL,
  c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
- Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
- Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
- Filtr URL musi uwzględniać komunikację po protokole HTTPS.
- Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
- Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
- Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

UWIERZYTELNIANIE

- Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
  a. lokalną bazę użytkowników (wewnętrzny LDAP),
  b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),

c. usługę katalogową Microsoft Active Directory.
- Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
- Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
  a. SSL,
  b. Radius,
  c. Kerberos.
- Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
- Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
- Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
- Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
- Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
- Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

- Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
- Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
  a. równoważenie względem adresu źródłowego,
  b. równoważenie względem połączenia.
- Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
- Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
- Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
- W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
- Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

- Urządzenie ma umożliwiać statyczne trasowanie pakietów.
- Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
- Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).

- Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

ADMINISTRACJA URZĄDZENIEM

- Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
- Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
- Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
- Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
- Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
- Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
- Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
- Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
- Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
- Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
- Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
- Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
- System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
- Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
- Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
- Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
- Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
  a. manualnego eksportu do pliku w dowolnym momencie czasu,
  b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
- Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
- Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
- Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

- Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
- System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
- System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
- System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
- System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
- System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
- Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
- Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
- Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

- Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
- Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
- Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
- Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
- Urządzenie ma posiadać usługę DNS Proxy.
- Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
- Urządzenie musi mieć zaimplementowane Open API
- Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
- Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
- Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.

GWARANCJA I SERWIS

- Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
- W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
- Urządzenie ma być objęte rozszerzoną gwarancją typu NBD tzn. w przypadku zgłoszenia awarii urządzenia, wysyłka urządzenia zastępczego lub wysyłka sprawnego urządzenia musi nastąpić

w dniu potwierdzenia awarii, a dostawa takiego urządzenia na wskazany przez zgłaszającego adres zaplanowana zostanie na kolejny dzień roboczy. Posiadanie rozszerzonej gwarancji NBD musi zostać potwierdzone licencją dystrybutora/producenta. Podmiot realizujący rozszerzoną gwarancję NBD musi posiadać certyfikat bezpieczeństwa informacji ISO27001 lub równoważny.

PARAMETRY SPRZĘTOWE

- Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
- Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
- Liczba portów Ethernet 2,5Gbps – min. 8.
- Liczba portów światłowodowych 1Gbps – min. 1.
- Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
- Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
- Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps.
- Przepustowość filtrowania Antywirusowego – minimum 500Mbps.
- Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.
- Maksymalna liczba tuneli VPN IPSec – minimum 100.
- Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.
- Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
- Obsługa interfejsów 802.11q (VLAN) – minimum 128
- Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.
- Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
- Urządzenie nie ma limitu na liczbę użytkowników.
- Liczba reguł filtrowania – minimum 8 192.
- Liczba tras statycznego routingu – minimum 512.
- Liczba tras dynamicznego routingu – minimum 10 000.
- Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
- Urządzenie musi być wyposażone w moduł TPM.

5. Dyski SSD SAS do macierzy dyskowej - 6 szt

Zamawiający posiada macierz dyskową DELL PowerVault ME5024 service tag D4YXWZ3.W ramach rozszerzenia przestrzeni dyskowej pod systemy virtual appliance zapewniające monitorowanie i zarządzenie systemem antywirusowym oraz gromadzeniem logów z infrastruktury urzędu oczekuje dostawy 6 sztuk dysków SSD o wielkości 1,92 TB SAS 24Gbps 2,5 cala Hot-Plug do intensywnego odczytu wraz ramkami montażowymi kompatybilnych z posiadaną macierzą Dyski muszą być nowe z gwarancją min 5 lat z opcją pozostawienia uszkodzonych dysków u Zamawiającego. Dostarczone dyski nie mogą powodować wadliwego działania macierzy będącej w posiadaniu zamawiającego oraz nie mogą pociągać ze sobą utraty gwarancji producenta tej macierzy.

IV. SPOSÓB PRZYGOTOWANIA I ZŁOŻENIA INFORMACJI

1. Informacje należy złożyć do **25.10.2024 r.** na formularzu ofertowym w następujący sposób:
a) elektronicznie na adres zamówieniapubliczne@ksiezpol.pl
b) osobiście lub listownie w formie oryginału na adres Urząd Gminy Księżpol ul. Biłgorajska 12, 23-415 Księżpol pierwsze piętro Sekretariat pokój nr 1
2. Ceny w informacji dotyczącej wartości zamówienia należy podać w walucie polskiej (PLN – polskich złotych).
3. Ceny w informacji dotyczącej wartości zamówienia musi obejmować wszystkie koszty, jakie poniesie Wykonawca w związku z realizacją przedmiotu zamówienia
4. Osobami upoważnionymi do kontaktów ze strony Zamawiającego jest Adrian Kapka, adres email: akapka@ksiezpol.pl, telefon: (84) 687 74 20 wew. 77
5. W celu zapewnienia porównywalności danych, Zamawiający zastrzega sobie prawo do kontaktowania się z Wykonawcami w celu uzupełnienia lub doprecyzowania złożonych propozycji

V. KLAUZULA INFORMACYJNA – RODO

Zgodnie z art. 13 ust. 1 i 3 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. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

1. Administratorem Pani/Pana danych osobowych jest Wójt Gminy Księżpol ul. Biłgorajska 12, 23-415 Księżpol tel. 84 6877420; fax 84 6877432; e-mail info@ksiezpol.pl;
2. W sprawach związanych z przetwarzaniem danych osobowych można kontaktować się z Inspektorem ochrony danych osobowych: tel. 604521364; mail: biuro@myszkowiak.pl
3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego prowadzonym w trybie przetargu podstawowego oraz w celu archiwizacji i przeprowadzanych kontroli;
4. Podstawę prawną przetwarzania danych osobowych stanowi ustawa Prawo zamówień publicznych. 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.
5. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18-19 oraz 74 -76 ustawy Pzp.
6. Pani/Pana dane osobowe będą przechowane, zgodnie z art. 78 ust. 1 Pzp przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy, oraz przez okres wynikający z przepisów szczególnych dotyczących archiwizacji. Okresy te dotyczą również Wykonawców, którzy złożyli oferty i nie zostały one uznane, jako najkorzystniejsze (nie zawarto z tymi Wykonawcami umowy).

7. W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO.
8. Posiada Pani/Pan prawo:
   1) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   2) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych[1];
   3) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO[2];
   4) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
9. Nie przysługuje Pani/Panu:
   1) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
   2) 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.

Z up. WÓJTA
mgr Adam Blicharz
ZASTĘPCA WÓJTA

Księżpol, dn. 17-10-2024 r. .....

Podpis Kierownika Zamawiającego lub osoby upoważnionej

Załączniki:

1. Formularz wyceny cenowej.

[1] Skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników

[2] Prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.