

Znak Sprawy: ZP.272.7.2023

Góra dnia 13.04.2023r.

Zapytanie ofertowe

ZAMAWIAJĄCY

Powiat Górowski

ul. Mickiewicza 1, 56-200 Góra

Numer telefonu 65 5443920

NIP: 693-19-57-453

Regon: 411 050 468

e-mail: sekretariat@powiatgora.pl

TRYB UDZIELENIA ZAMÓWIENIA

Powiat Górowski zgodnie z art. 44 ust. 3 ustawy z dnia 29 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2022, poz. 1634 ze zm.) zaprasza do złożenia oferty na: „Cyfrowy Powiat- Zakup sprzętu”.

W związku z faktem, że wartość szacunkowa zamówienia nie przekracza kwoty 130 000 zł netto, zamówienie prowadzone jest z wyłączeniem przepisów ustawy Prawo zamówień publicznych.

1. Przedmiot zamówienia:

„Cyfrowy Powiat- Zakup sprzętu”.

Kod CPV 30200000-1: Urządzenia komputerowe

Kod CPV 30213300-8: Komputer biurowy

Kod CPV 30237200-1: Akcesoria komputerowe

2. TERMIN REALIZACJI ZAMÓWIENIA

do 15.05.2023 r.

3. OPIS KRYTERIÓW ORAZ SPOSÓB OCENY OFERT:

a. Przy wyborze ofert Zamawiający będzie się kierował następującymi kryteriami:

1 kryterium: cena - waga 100%

Sposób oceny ofert:

najniższa cena brutto

ilość punktów = $\frac{\text{cena brutto danej oferty}}{\text{cena brutto danej oferty}}$ x 100 = ilość otrzymanych pkt

cena brutto danej oferty

Za ofertę najkorzystniejszą uznana zostanie oferta, która uzyska największą ilość punktów.

4. OPIS SPOSOBU PRZYGOTOWYWANIA OFERT

4.1 Wykonawca może złożyć tylko jedną ofertę zgodnie ze wzorem formularza oferty (zał. nr 1)

4.2. Do oferty należy załączyć następujące dokumenty:

- formularz ofertowy (załącznik nr 1).
- opis przedmiotu zamówienia (załącznik nr 2).
- wzór umowy (załącznik nr 3).
- klauzula informacyjna (załącznik nr 4).

5. MIEJSCE I TERMIN SKŁADANIA OFERTY

- a. Oferty należy złożyć do **21.04.2023r do godziny 10:00** w formie: pocztą elektroniczną na adres: <https://platformazakupowa.pl/pn/powiatgora>

6. TERMIN OTWARCIA OFERT.

- a. Termin otwarcia ofert **21.04.2023r do godziny 10:30**

INFORMACJE DODATKOWE:

- a/ Zamawiający zastrzega sobie prawo do unieważnienia niniejszego postępowania bez podania uzasadnienia, a także do pozostawienia postępowania bez wyboru oferty.
- b/ Zamawiający nie przewiduje zwrotu kosztów postępowania.
- c/ Zamawiający nie dopuszcza składania ofert częściowych.
- d/ Wykonawca może złożyć tylko jedną ofertę zgodną z zapytaniem.
- e/ Zamawiający wymaga, aby Wykonawca składając ofertę uwzględnił wszystkie pozycje określone w zapytaniu ofertowym i Warunkach technicznych
- f/ Jeżeli w niniejszym postępowaniu nie będzie można dokonać wyboru najkorzystniejszej oferty ze względu na to, że zostały złożone oferty o takiej samej cenie, Zamawiający zastrzega sobie możliwość wezwania do złożenia oferty dodatkowej.
- g/ Złożenie oferty nie zapewnia uzyskania zlecenia na wykonanie w/w zamówienia.
- h/ Osoba upoważniona do kontaktu z Wykonawcami – Andrzej Rybak, , e-mail: a.rybak@powiatgora.pl
- i/ Informacja z wyboru Wykonawcy zostanie podana Oferentom pocztą elektroniczną.

Załączniki:

- formularz ofertowy (załącznik nr 1).
- Specyfikacja techniczna urządzenia (załącznik nr 2).
- wzór umowy (załącznik nr 3).
- klauzula informacyjna (załącznik nr 4).

Z up. STAROSTY
.....
Andrzej Rogala
WICESTAROSTA

SPECYFIKACJA TECHNICZNA -OPIS PRZEDMIOTU ZAMÓWIENIA

Sprzęt musi być zgodny, równoważny lub o wyższych parametrach technicznych z wymaganiami określonymi poniżej:

1. Komputer stacjonarny z monitorem (15 szt.)

Nazwa	Minimalne wymagania dla sprzętu
Zastosowanie	Zestaw komputerowy będzie wykorzystywany dla potrzeb aplikacji biurowych, obsługi systemów dziedzinowych, dostępu do Internetu oraz poczty elektronicznej. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji u producenta komputera.
Monitor	a) minimum 23,8", max 24,5", matowy o rozdzielczości minimum 1920 x 1080 FHD b) jasność minimum 250 cd/m ² c) odświeżanie min. 75Hz d) technologia matrycy IPS e) rodzaj podświetlenia LED f) czas reakcji min. 4ms g) kąt widzenia w pionie 178° h) kąt widzenia w poziomie 178° i) złącza: minimum 2 x HDMI j) wbudowane głośniki k) minimum 3-letnia gwarancja producenta Door-to-Door
KOMPUTER	
Procesor	Procesor musi osiągać w rankingu PassMark CPU Mark co najmniej 19,548 punktów na dzień 27.03.2023. (wynik dostępny pod adresem: https://www.cpubenchmark.net/high_end_cpus.html)
Pamięć RAM	Minimum 16 GB, możliwość rozbudowy do 64GB,
Pamięć masowa	Minimum 256 GB SSD M.2 PCIe

	<p>Dysk twarde musi zawierać partycję recovery,</p> <p>Partycja musi zapewniać przywrócenie systemu operacyjnego</p>
Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia pamięci.
Napęd optyczny	Nagrywarka DVD +/-RW
Wyposażenie	<p>a) Karta dźwiękowa zintegrowana z płytą główną,</p> <p>b) Zintegrowana karta sieciowa Gigabit Ethernet RJ 45,</p> <p>c) WiFi minimum 802.11 a/b/g/n/ac,ax,</p> <p>d) Zintegrowany układ szyfrujący Trusted Platform Module,</p> <p>e) Co najmniej 8 złącza USB, 4 porty na panelu przednim, 4 na panelu tylnym; wymagana ilość portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.</p> <p>f) Porty audio: przedni panel wejście na mikrofon, wyjście na słuchawki - dopuszcza się rozwiązania combo, tylny panel: wyjście liniowe</p> <p>g) 1x HDMI, 1x DisplayPort</p>
Zasilanie	Zasilacz wbudowany, o mocy min. 180W
Obudowa	<p>a) musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona)</p> <p>b) założona blokada Kensington musi uniemożliwiać otworzenie tylnej obudowy</p> <p>c) typ obudowy Mini Tower</p>
Wymagania dodatkowe	<p>Komputer musi posiadać dostęp do aktualizacji systemu BIOS, podręczników użytkownika, najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta komputera numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony.</p> <p>Komputer musi posiadać możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera.</p> <p>Do oferty należy dołączyć kartę katalogową/specyfikację techniczną urządzenia. Karta powinna zawierać wyraźne zdjęcia obudowy oferowanego komputera.</p> <p>Klawiatura USB kolorystycznie zgodna z całym zestawem komputerowym, klawiatura z wydzielonym blokiem numerycznym.</p> <p>Mysz optyczna min. 800 dpi, USB z dwoma przyciskami oraz rolką</p>

Bezpieczeństwo	<p>Komputer musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowym tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe.</p> <p>BIOS zgodny ze specyfikacją UEFI - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: - nr seryjnym, wersja oraz nazwa komputera - ilości pamięci RAM</p> <p>- typie procesora,</p> <p>Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) · Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń · Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego.</p> <p>Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. · Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.</p>
System operacyjny	<p>Zainstalowany system operacyjny: MS Windows 11 Pro. PL 64-bit lub Windows 10 Pro z możliwością aktualizacji do wersji 11</p> <p>Licencja systemu operacyjnego zaimplementowana w BIOS komputera, umożliwiająca instalację systemu bez podawania klucza oraz bez aktywacji systemu za pośrednictwem Internetu.</p> <p>Nie dopuszcza się zaferowania systemu operacyjnego typu refurbished.</p>
Certyfikaty	<p>Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty)</p> <p>Deklaracja zgodności CE (załączyć do oferty)</p> <p>Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki.</p>
Uruchomienie i konfiguracja	<ol style="list-style-type: none"> 1. Uruchomienie w siedzibie zamawiającego dostarczonego sprzętu komputerowego w celu przetestowania poprawności działania 2. Instalacja podstawowego oprogramowania (Adobe Reader, 7zip, Mozilla Firefox, program antywirusowy wskazany przez zamawiającego)
Warunki gwarancji	<p>Minimum 3-letnia gwarancja producenta.</p>

Oferowany model komputera	
Oferowany model monitora	

Cena brutto za 1 szt. zestawu	
Cena brutto za 15 szt. zestawu	

2. Zasilacz awaryjny ups (15 szt.)

Nazwa	Minimalne wymagania dla sprzętu
Moc	750VA / 450W
Bateria	12V/7Ah lub 12V/9Ah
Gniazda	6 gniazd wyjściowych: 3 z podtrzymaniem baterijnym, 3 z ochroną przeciwprzebiegową
Zabezpieczenia	Ograniczenie prądowe przy pracy z sieci jak i z akumulatora, zabezpieczenie przed zbyt głębokim rozładowaniem
Inne	Zimny start (możliwość uruchomienia z baterii)

Oferowany model	
Cena brutto za 1 szt.	
Cena brutto za 15 szt.	

3. Urządzenie wielofunkcyjne (3 szt.)

Nazwa	Minimalne wymagania dla sprzętu
Rodzaj wydruku	A4, monochromatyczny, laserowy
Funkcje	Drukowanie, skanowanie, kopiowanie
Oryginalny podajnik	50 arkuszy A4 (standard, A6R-A4), 50-160 g / m ² , (z funkcją podwójnego skanowania)
Szybkość kopiowania	maks. 40 stron A4 / min, dupleks: maks. 20 stron A4 / min
Pierwsza strona / czas nagrzewania	6,4 sekundy * (kopiowanie / drukowanie), 17 sekund)
Rozdzielczość kopiowania	600 x 600 dpi

Funkcje inne	Dupleks, rezerwacja zadań, funkcja programu, kopiowanie dokumentów tożsamości, skanowanie ciągle, pomijanie pustych stron, N-stron, tryb cichy (tryb połowy prędkości), 100 kodów zarządzania
Interfejsy	USB 2.0, 10/100 / 1000BaseTX, host USB, gniazdo SD
Skanowanie	Skanowanie do SMB, skanowanie do wiadomości e-mail, skanowanie do FTP, skanowanie TWAIN, skanowanie WIA, uwierzytelnianie SMTP, LDAP
Bęben światłoczuły	Wbudowany w toner lub wyodrębniony (o wydajności około 100 tys. stron)

Oferowany model	
Cena brutto za 1 szt.	
Cena brutto za 3 szt.	

4. Urządzenie brzegowe UTM z obsługą skanera antywirusowego

Nazwa/Cecha	Minimalne wymagania
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
Ochrona antywirusowa	<ul style="list-style-type: none"> • 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 antyspamowa	<ul style="list-style-type: none"> • Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). • Ochrona antyspam ma działać w oparciu o białe/czarne listy, DNS RBL, 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.
Firewall	<ul style="list-style-type: none"> • 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

	<p>źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.</p> <ul style="list-style-type: none"> • 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 (wewnętrzna oraz zewnętrzna), 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.
<p style="text-align: center;">IPS</p>	<ul style="list-style-type: none"> • 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. • Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
<p style="text-align: center;">Kształtowanie pasma</p>	<ul style="list-style-type: none"> • 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.
<p style="text-align: center;">Wirtualne sieci prywatne</p>	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> 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.
<p style="text-align: center;">Filtr dostępu do stron www</p>	<ul style="list-style-type: none"> • 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

	<p>danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:</p> <ol style="list-style-type: none"> blokowanie dostępu do adresu URL, zezwoleń na dostęp do adresu URL, blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. <ul style="list-style-type: none"> 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 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	<ul style="list-style-type: none"> Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: <ol style="list-style-type: none"> lokalną bazę użytkowników (wewnętrzny LDAP), zewnętrzną bazę użytkowników (zewnętrzny LDAP), 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: <ol style="list-style-type: none"> SSL, Radius, 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. 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 ISP	<ul style="list-style-type: none"> Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy: <ol style="list-style-type: none"> równoważenie względem adresu źródłowego, 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 niezasyfrowany 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

	<p>(także nakładającymi się) uprawnieniami.</p> <ul style="list-style-type: none"> • 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 zarządzania 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 zapisywanie logów na wbudowanym dysku. • 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: <ul style="list-style-type: none"> 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.
<p style="text-align: center;">Raportowanie</p>	<ul style="list-style-type: none"> • 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).
<p style="text-align: center;">Pozostałe</p>	<ul style="list-style-type: none"> • 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.

	<ul style="list-style-type: none"> • 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 podłączenie karty SD w celu zapisywania logów. • Liczba portów Ethernet 10/100/1000Mbps – min.8. • Urządzenie ma umożliwiać dostęp do Internetem 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 2.4Gbps. • Przepustowość filtrowania Antywirusowego – minimum 495Mbps. • Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 600Mbps. • Maksymalna liczba tuneli VPN IPSec – minimum 100. • Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 20. • 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 18 000 nowych sesji/sekundę. • Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. • Urządzenie nie może posiadać limitu na liczbę użytkowników.
--	---

Oferowany model	
Cena brutto	

Dodatkowe wymagania (dotyczy wszystkich urządzeń opisanych w zamówieniu)

1. Sprzęt komputerowy musi być fabrycznie nowy.
2. Sprzęt musi być dostarczony, rozpakowany i uruchomiony w siedzibie Zamawiającego oraz jednostkach organizacyjnych wskazanych przez Zamawiającego.
3. W przypadku zgłoszenia usterki dowolnego urządzenia objętego gwarancją Wykonawca zobowiązany jest w ciągu 48 godzin od chwili zgłoszenia do oceny problemu w miejscu eksploatacji urządzenia oraz podjęcia działań związanych z naprawą gwarancyjną.
4. W przypadku gdy naprawa urządzenia nie będzie wykonywana w miejscu jego eksploatacji Wykonawca zobowiązany jest do odebrania uszkodzonego urządzenia i jego zwrotnego dostarczenia po naprawie na swój koszt.

Z up.: STAROSTY.....
Andrzej Rogula
WICESTAROSTA

.....
Pieczęć wykonawcy**Dane dotyczące oferenta**

Nazwa.....
 Siedziba.....
 Nr telefonu/faks.....
 e-mail

NIP..... REGON..... KRS.....

FORMULARZ OFERTOWY

Nawiązując do zapytania ofertowego Powiatu Górowskiego na „Cyfrowy Powiat- Zakup sprzętu”.
 Składamy niniejszą ofertę.

Oferuję realizację zamówienia w zakresie określonym w zapytaniu ofertowym za cenę:

*** Niepotrzebne skreślić**

1. *Komputer stacjonarny z monitorem*
 cena jednostkowa brutto zł
 cena (15 szt.) netto zł
 VAT %
 cena brutto zł
 (słownie złotych: 100)

2. *Zasilacz awaryjny ups*
 cena jednostkowa brutto zł
 cena (15 szt.) netto zł
 VAT %
 cena brutto zł
 (słownie złotych: 100)

3. *Urządzenie wielofunkcyjne (3 szt.)*
 cena jednostkowa brutto zł
 cena (3 szt.) netto zł
 VAT %
 cena brutto zł
 (słownie złotych: 100)

4. *Urządzenie brzegowe UTM z obsługą skanera antywirusowego*
 cena netto zł
 VAT %
 cena brutto zł
 (słownie złotych: 100)

Wartość ogółem

cena netto zł
VAT %
cena brutto zł
(słownie złotych: 100)

Jednocześnie oferuję:

- termin płatności faktury: 30 dni

Oświadczamy, że:

1. Zapoznałem/am się z treścią zapytania ofertowego i akceptuję jego postanowienia.

2. Zapoznałem/am się z treścią wzoru umowy i w przypadku wyboru mojej oferty zobowiązuję się podpisać umowę na warunkach w nim określonych.
3. Termin wykonania zamówienia;
Do 15.05.2023 r.
4. Termin związania ofertą: 30 dni od daty składania ofert.
5. Oświadczamy, że zapoznaliśmy się z przedmiotem zamówienia i nie wnosimy do niego żadnych zastrzeżeń.
6. Oświadczamy, że posiadamy uprawnienia, wiedzę i doświadczenie niezbędne do wykonania zamówienia.
7. Osobą (do realizacji zadania) ze strony Wykonawcy upoważnianą do kontaktów jest _____, tel. _____.
8. adres e-mail: _____.
9. Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy 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 oświadczenia tego wykonawca nie składa - należy usunąć treść oświadczenia np. poprzez jego wykreślenie).

.....
(miejscowość i data)

PROJEKT UMOWY nr ZP.272.7.2023

zawarta w dniu2023 r. w Górze pomiędzy:
Powiatem Górowskim reprezentowanym przez:

- Starostę Górowskiego - Urszulę Szmydyńską
 - Wicestarostę Górowskiego - Andrzeja Rogalę
- przy kontrasygnacie
- Skarbnika Powiatu - Wiesława Pospiecha

zwanym dalej w treści umowy „Zamawiającym”,
a:

.....
.....
NIP:, Regon:
reprezentowanym przez

.....
zwanym dalej w treści umowy „Wykonawcą”,
na podstawie dokonanego przez zamawiającego wyboru oferty wykonawcy w trybie zapytania ofertowego.

Przedmiot niniejszej umowy: „Cyfrowy Powiat- Zakup sprzętu” jest: zgodny z zapytaniem ofertowym.

§ 1

1. Na podstawie niniejszej umowy Wykonawca zobowiązuje się do wykonania na rzecz Zamawiającego dostawy sprzętu.
2. Sprzęt komputerowy musi być fabrycznie nowy.
3. Sprzęt musi być dostarczony, rozpakowany i uruchomiony w siedzibie Zamawiającego oraz jednostkach organizacyjnych wskazanych przez Zamawiającego.

§ 2

1. Wykonawca udziela gwarancji na przedmiot zamówienia: na 36 miesięcy. Gwarancja polega na:
2. W przypadku zgłoszenia usterki dowolnego urządzenia objętego gwarancją Wykonawca zobowiązany jest w ciągu 48 godzin od chwili zgłoszenia do oceny problemu w miejscu eksploatacji urządzenia oraz podjęcia działań związanych z naprawą gwarancyjną.
3. W przypadku gdy naprawa urządzenia nie będzie wykonywana w miejscu jego eksploatacji Wykonawca zobowiązany jest do odebrania uszkodzonego urządzenia i jego zwrotnego dostarczenia po naprawie na swój koszt.

§ 3

1. Wykonawca oświadcza, że przed podpisaniem umowy zapoznał się z miejscem wykonania przedmiotu umowy, warunkami technicznymi, a także otrzymał od Zamawiającego wszelkie żądane wyjaśnienia i nie wnosi w tym zakresie żadnych uwag i zastrzeżeń.

2. Wykonawca ponosi pełną odpowiedzialność za szkodę powstałą w wyniku zaniedbań w wykonywaniu obowiązków określonych niniejszą umową, jak również za szkody powstałe na skutek ich niewykonania. Ponadto Wykonawca ponosi odpowiedzialność za działania i zaniechania swoich pracowników w związku z wykonywaniem przez nich przedmiotu zamówienia jak za swoje własne i w razie powstania szkody zobowiązany jest do jej naprawienia.

3. Wykonawca nie ponosi odpowiedzialności za wadliwe funkcjonowanie urządzeń i instalacji wynikające z:

- a) niewłaściwej obsługi,
- b) napraw dokonywanych przez inne niż uprawnione przez Wykonawcę osoby ,
- c) fizycznego zużycia elementów/uszkodzeń elementów powstałych w następstwie wyładowań atmosferycznych oraz przepięć w sieci energetycznej.

4. Jeżeli w trakcie realizacji przedmiotu umowy zaistnieje konieczność rozszerzenia zakresu prac o prace niemożliwe do przewidzenia przed zawarciem umowy, prace takie będą wykonane tylko w ramach niniejszej umowy i w kwocie ustalonej w niniejszej umowie (wynagrodzenie ryczałtowe).

§ 4

1. Za wykonanie przedmiotu umowy Zamawiający zapłaci Wykonawcy wynagrodzenie określone w formularzu oferty, ustalone na

kwotę zł netto,
słownie; złotych /100,
podatek 23% VAT zł.
słownie: złotych ... /100,
kwotę zł brutto,
słownie: złotych /100.

2. Zamawiający przewiduje płatność za przedmiot zamówienia w jednej fakturze – za zrealizowanie zamówienia , o którym mowa w § 1

3. Podstawę wystawienia faktury stanowi załączony protokół odbioru.

4. Wynagrodzenie za wykonane prace będzie płatne przelewem w terminie do 30 dni od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury. Należność przekazana będzie na rachunek bankowy Wykonawcy wskazany w treści faktury.

5. Wynagrodzenie, o którym mowa w niniejszym paragrafie zawiera wszelkie koszty niezbędne do prawidłowego wykonania przedmiotu umowy w okresie obowiązywania umowy.

6. Za datę zapłaty strony przyjmują datę obciążenia rachunku bankowego Zamawiającego.

§ 5

1. Przedstawiciele Zamawiającego :

a/ Sekretarz Powiatu nr tel. 65 5443903

e-mail: organizacyjny@powiatgora.pl

2. Przedstawiciele Wykonawcy:

a/ ze Strony Wykonawcy –, tel.

e-mail:

§ 6

1. Wykonawca zapłaci Zamawiającemu karę umowną:

a) za zwłokę w wykonaniu przedmiotu umowy w wysokości 0,5% całkowitego wynagrodzenia brutto określonego w § 4 ust.1 za każdy dzień zwłoki po terminie realizacji przedmiotu zamówienia.

b) za zwłokę w usunięciu usterek stwierdzonych przy odbiorze w wysokości 0,5% całkowitego wynagrodzenia brutto za każdy dzień opóźnienia liczonej od dnia wyznaczonego na usunięcie usterek,

c) za zwłokę Wykonawcy w wymianie wadliwego urządzenia w wysokości 0,5% całkowitego wynagrodzenia brutto określonego w § 4 ust.1 za każdy dzień opóźnienia,

d) w przypadku nie dotrzymania warunków gwarancji, określonych § 2, Wykonawca zapłaci w wysokości 0,5% wynagrodzenia brutto określonego w § 4 ust.1 za każdy dzień opóźnienia,

e) za odstąpienie Zamawiającego w całości lub części umowy z przyczyn zależnych od Wykonawcy w wysokości 10% całkowitego wynagrodzenia brutto określonego w § 4 ust.1.

2.Kary należne Zamawiającemu będą płatne przez Wykonawcę w terminie 7 dni od daty wystawienia przez Zamawiającego noty obciążeniowej lub z faktury Wykonawcy. Zamawiający zastrzega sobie prawo potrącenia kar umownych z wynagrodzenia Wykonawcy poprzez dokonanie zapłaty w kwocie odpowiednio niższej w stosunku do zobowiązania wynikającego z faktury na podstawie noty obciążeniowej. O ile powyższe okaże się niemożliwe zapłata kar umownych zostanie dokonana na wezwanie przekazane Wykonawcy przez Zamawiającego w terminie 7 dni od wezwania.

3.Strony zastrzegają sobie prawo do odszkodowania uzupełniającego, przekraczającego wysokość kar umownych, do wysokości rzeczywiście poniesionej szkody na zasadach ogólnych.

4. Łączna maksymalna wysokość kar umownych nie może przekroczyć 20 % wartości wynagrodzenia brutto określonego w § 4 ust. 1 umowy.

§ 7

Termin realizacji przedmiotu zamówienia do 15.05.2023 r.

§ 8

1.Zmiany i uzupełnienia umowy mogą nastąpić za zgodą Stron wyrażoną w formie pisemnej pod rygorem nieważności i dopuszczalne są w ramach uregulowań zapisanych w niniejszej umowie oraz Zapytaniu ofertowym.

2.Odstąpienie od umowy powinno nastąpić w formie pisemnej pod rygorem nieważności i powinno zawierać uzasadnienie.

§ 9

1.Zamawiający nie wyraża zgody na przeniesienie wierzytelności wynikających z niniejszej umowy na osoby trzecie.

2.Wszelkie zmiany i uzupełnienia wymagają formy pisemnej pod rygorem nieważności.

3.W sprawach nieuregulowanych niniejszą umową obowiązują przepisy Kodeksu Cywilnego oraz inne właściwe.

4.Ewentualne spory wynikłe w trakcie realizacji niniejszej umowy będzie rozstrzygał sąd właściwy dla siedziby Zamawiającego.

5.Strony zobowiązują się wzajemnego do informowania o istotnych zmianach dotyczących realizacji umowy.

6.Umowę sporządzono w trzech jednobrzmiących egzemplarzach, w tym dwa egzemplarze dla Zamawiającego i jeden dla Wykonawcy.

ZAMAWIAJĄCY:

WYKONAWCA:

.....

.....

.....

Klauzula informacyjna ZP-3. Zamówienia publiczne o wartości nie przekraczającej kwoty 130 000 złotych.

POWIAT GÓROWSKI

56-200 Góra, ul. Mickiewicza 1
tel. 65-544-39-00 fax 65-543-35-11
NIP 6931957453 Regon: 411050468



Na podstawie art. 13 ust. 1 i 2 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 4.05.2016), zwanego dalej RODO informujemy, że:

1. Administratorem Pani/Pana danych osobowych jest Starostwo Powiatowe w Górze reprezentowane przez Starostę Górowskiego, z siedzibą w: 56-200 Góra ul. Adama Mickiewicza 1, NIP: 693-18-38-688, Regon: 411 116 871, tel. 65/544 39 00, e-mail: sekretariat@powiatgora.pl

2. Inspektorem ochrony danych w Starostwie Powiatowym w Górze jest Tomasz Wadas. W sprawach związanych z danymi osobowymi można się kontaktować z Inspektorem ochrony danych w Starostwie Powiatowym w Górze pod adresem e-mail: iod@powiatgora.pl

3. Pani/Pana dane osobowe przetwarzane będą :
- na etapie postępowania o udzielenie zamówienia zgodnie z art. 6 ust. lit. c) RODO oraz przepisów ustawy z dnia 27 sierpnia 2009r. o finansach publicznych
- na etapie zawierania umowy zgodnie z art. 6 ust. 1 lit. b) RODO w celu zawarcia i prawidłowego wykonania umowy,

4. W związku z przetwarzaniem danych w celach o których mowa w pkt 3 odbiorcami Pani/Pana danych osobowych mogą być podmioty uprawnione na podstawie przepisów prawa lub umowy powierzenia przetwarzania danych. Zgodnie z przepisami prawa dane publikowane będą na stronie internetowej Biuletynu Informacji Publicznej Administratora,

5. Pani/Pana dane osobowe będą przechowywane, przez czas wymagany przepisami prawa tj. realizacji postępowania o udzielenie zamówienia publicznego, a po tym czasie zgodnie z przepisami dotyczącymi archiwizacji,

6. Pani/Pana dane osobowe nie będą podlegały zautomatyzowanym procesom podejmowania decyzji, w tym profilowaniu,

7. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego ani do organizacji międzynarodowej,

8. Podanie danych jest obowiązkowe i jest wymogiem ustawowym. W przypadku niepodania danych nie będzie możliwy udział w postępowaniu o udzielenie zamówienia publicznego, Prawa osoby, które dane są przetwarzane

9. W związku z przetwarzaniem Pani/Pana danych osobowych na podstawie art. 6 ust. 1 lit. c) przysługują Pani/Panu następujące prawa:
a) prawo dostępu do treści swoich danych osobowych;
b) prawo do żądania sprostowania (poprawienia) danych osobowych ;[1]
d) prawo do ograniczenia przetwarzania z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;[2]

10. Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego właściwego w sprawach ochrony danych osobowych tj. Prezesa Urzędu Ochrony Danych Osobowych (PUODO), ul. Stawki 2, 00-193 Warszawa, tel. 22 531 03 00.

Z up. STAROSTY

Andrzej Rogala
WICESTAROSTA

Nazwa firmy:

.....
.....
.....

Adres:

.....
.....
.....

OŚWIADCZENIE

o wykonaniu obowiązków informacyjnych na podstawie art. 13 i 14 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

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO¹ wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu ² pn.: **Cyfrowy Powiat- Zakup sprzętu.**

czytelny podpis i pieczęć firmy

¹ Rozporządzenie 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).

² 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 treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).