

ZAPYTANIE OFERTOWE

**na dostawę sprzętu komputerowego i oprogramowania,
przeprowadzenie diagnozy cyberbezpieczeństwa,
przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa, wykonanie audytu KRI
wraz z poprawą procedur systemów zarządzania bezpieczeństwem
w Urzędzie Miasta i Gminy Bolimów w ramach projektu grantowego „Cyfrowa Gmina”.**

Nr sprawy: GRP.7011.67.2022

Postępowanie o udzielenie zamówienia prowadzone zgodnie z zasadą konkurencyjności.

Zatwierdzam:

Bolimów, 2022-07-04

Spis treści

ROZDZIAŁ 1. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO.	3
ROZDZIAŁ 2. TRYB UDZIELENIA ZAMÓWIENIA.	3
ROZDZIAŁ 3. OPIS PRZEDMIOTU ZAMÓWIENIA.	3
ROZDZIAŁ 4. TERMIN REALIZACJI UMOWY.	24
ROZDZIAŁ 5. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCENY ICH SPEŁNIENIA.	25
ROZDZIAŁ 6. PRZESŁANKI WYKLUCZENIA.	25
ROZDZIAŁ 7. WYKAZ OŚWIADCZEŃ I DOKUMENTÓW, POTWIERDZAJĄCYCH SPEŁNIANIE WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ BRAK PODSTAW DO WYKLUCZENIA.	26
ROZDZIAŁ 8. INFORMACJA DLA WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA.	27
ROZDZIAŁ 9. INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ I DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI.	28
ROZDZIAŁ 10. OPIS SPOSOBU PRZYGOTOWYWANIA OFERTY.	29
ROZDZIAŁ 11. MIEJSCE, SPOSÓB ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT.	30
ROZDZIAŁ 12. OPIS SPOSOBU OBLICZENIA CENY.	31
ROZDZIAŁ 13. OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT..	32
ROZDZIAŁ 14. OCENA I WYBÓR OFERTY.	32
ROZDZIAŁ 15. ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI ZAWIERANEJ UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO ORAZ WARUNKI ISTOTNE ZMIANY UMOWY.	33
ROZDZIAŁ 16. UNIEWAŻNIENIE POSTĘPOWANIA.	36
ROZDZIAŁ 17. POZOSTAŁE INFORMACJE.	36
ROZDZIAŁ 18. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH W PROGRAMIE CYFROWA POLSKA 2014-2020 (POPC 2014-2020).	37
ROZDZIAŁ 19. KLAUZULA INFORMACYJNA Z ART. 13 RODO.	39
ROZDZIAŁ 20. WYKAZ ZAŁĄCZNIKÓW.	40

ROZDZIAŁ 1. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO.

Nazwa i adres Zamawiającego:

Gmina Bolimów, zwana dalej Zamawiającym

ul. Łowicka 9, 99-417 Bolimów

nr telefonu: 46 838 03 05

strona internetowa: <https://bip.ugbolimow.nv.pl>

adres e-mail: ug.sekretariat@bolimow.pl

NIP 836-15-38-156, REGON 750147863

Godziny pracy Urzędu Miasta i Gminy: poniedziałek godz. 10.00-18.00, wtorek-

piątek godz. 7.30-15.30

Miejsce publikacji zapytania ofertowego:

Strona internetowa Zamawiającego: <https://bip.ugbolimow.nv.pl>

Strona internetowa wskazana w komunikacie ministra właściwego ds. rozwoju, przeznaczona do umieszczania zapytań ofertowych:

<https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl/>

Strona internetowa, na której udostępnianie będą dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia:

<https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl/>

<https://bip.ugbolimow.nv.pl>

ROZDZIAŁ 2. TRYB UDZIELENIA ZAMÓWIENIA.

- 2.1. Postępowanie prowadzone jest zgodnie z zasadą konkurencyjności określoną w „Wytyczne w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020” (Mlir/2014-2020/12(5)) dla postępowań o wartości przekraczającej kwotę 50 000 PLN netto, zwane w dalszej części zapytania „Wytycznymi”.
- 2.2. Niniejsze postępowanie nie podlega przepisom ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2021 r., poz. 1129 z późn. zm.) zgodnie z art. 2 ust. 1 pkt. 1 ustawy.

ROZDZIAŁ 3. OPIS PRZEDMIOTU ZAMÓWIENIA.

- 1) Przedmiotem zamówienia jest na dostawę sprzętu komputerowego i oprogramowania, przeprowadzenie diagnozy cyberbezpieczeństwa, przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa, wykonanie audytu KRI wraz z poprawą procedur systemów zarządzania bezpieczeństwem w Urzędzie Miasta i Gminy Bolimów w ramach projektu grantowego „Cyfrowa Gmina”.
- 2) Zamówienie zostało podzielone na 2 części:
 - 1) **część 1 zamówienia:** dostawa sprzętu komputerowego i oprogramowania dla Urzędu Miasta i Gminy Bolimów,
 - 2) **część 2 zamówienia:** przeprowadzenie diagnozy cyberbezpieczeństwa, przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa, wykonanie audytu KRI

wraz z poprawą procedur systemów zarządzania bezpieczeństwem w Urzędzie Miasta i Gminy Bolimów.

3) Część 1 zamówienia: Dostawa sprzętu komputerowego i oprogramowania dla Urzędu Miasta i Gminy Bolimów:

3.3.1. Serwer

Parametr	Minimalne wymagania
Procesor	min: 2 x Intel Xeon Silver 4210 (2,2GHz, 10 rdzeni/20 wątków, 9,6GT/s, 13,75MB pamięci podręcznej, Turbo, HT, 85W), DDR4-2400
RAM	min: 4 x 32GB pamięci RDIMM, 3200MT/s, moduły dwubankowe, podstawa 16GB x8
Dyski	min: 3 x 960GB SSD SATA 6Gb/s 512e 2,5" dysk do intensywnego odczytu wymieniany bez wyłączania systemu, S4510, 1 DWPD 1 x BOSS karta kontrolera z 1 kartą M.2 240GB (brak RAID), niskoprofilowa
Napęd	1 x DVD +/-RW napęd SATA wewnętrzny
Zasilanie	1 x Podwójny nadmiarowy zasilacz wymieniany bez wyłączania systemu (1+1), 550W
LAN	1 x Broadcom 5720 dwuportowa karta sieciowa Mezzanine LOM 1 GbE, 1 x Dwuportowa karta LOM 1GbE na płycie głównej
Dodatkowo	1 x Moduły RDIMM 3200MT/s 1 x 2.5" Chassis up to 8 HP HDDs,PERC/HBA11 1 x LCD Obudowa serwera 1 x iDRAC9 Enterprise 1 x Wewnętrzny kontroler PERC 1 x Karta PERC H750, niskoprofilowa 1 x Układ Trusted Platform Module 2.0
Oprogramowanie	1 x Windows Server 2022 Standard z licencją na wszystkie rdzenie
Konfiguracja serwera	Instalacja serwera w siedzibie Zamawiającego: – instalacja/konfiguracja usługi active directory – założenie kont użytkowników – konfiguracja podstawowych zasad GPO
Gwarancja	Next Business Day 36 miesięcy

3.3.2. Laptop

Parametr	Minimalne wymagania
Kolor produktu	Czarny
Wyświetlacz	15.6", 1920 x 1080 px, Full HD, WVA, LED, MATOWY
Jasność	220 cd/m ²
Procesor	Intel® Core™ i5 dziesiątej generacji i5-1035G1



Taktowanie procesora	1 GHz Maksymalne taktowanie procesora: 3,6 GHz
Liczba rdzeni procesora	4
Cache procesora	6MB
Pamięć	DDR4-SDRAM
Pamięć wewnętrzna	8GB
Prędkość zegara pamięci	2666 Mhz
Maksymalna pojemność pamięci	16GB
Nośnik danych	SSD NVMe,PCI Express, M.2
Całkowita pojemność przechowywania	256 GB
Obsługiwane typy kart pamięci	SDSDHCSDXC
Model karty graficznej on-board	Intel® UHD Graphics
Układ audio	Realtek ALC3204
Ilość wbudowanych głośników	2 o mocy 2W
Mikrofon	TAK
Kamera	TAK 0,92 MP, 1280 x 720 px
Sieć	
Bluetooth	TAK 5.1
Standardy Wi- Fi	Wi-Fi 6 (802.11ax)
Przewodowa sieć LAN	10/100/1000 Mbit/s
Porty i interfejsy	
Liczba portów USB 2.0	1
Ilość portów USB 3.2 Gen 1 (3.1 Gen 1) Typu-A	2
Ilość portów Ethernet LAN (RJ-45)	1
Ilość portów HDMI	1 – 1.4
Port dla zestaw słuchawka/mikrofon	TAK
Typ portu ładowania	DC-in Jack



Klawiatura	Amerykański międzynarodowa, numeryczna z podświetleniem
Zainstalowany system operacyjny	Windows 10Pro 64 bit
Bateria	Litowo-polimerowy (LiPo), 3 komory, 41Wh
Kensington Lock	TAK
Czytnik linii papilarnych	TAK
Waga produktu max	1,69kg
Gwarancja	36 miesięcy

3.3.3. Urządzenie wielofunkcyjne ze skanerem

Parametr	Minimalne wymagania
Rodzaj urządzenia	wielofunkcyjne - druk/skan/kopia
Technologia druku	atramentowa
Format	A4
Obsługa Bluetooth	TAK (BLE)
Standardowa pamięć	256 MB (DDR3)
Procesor	700 MHz
Poziom hałasu	max 57,2 dB
Rozdzielczość druku mono	1200x1200 dpi
Rozdzielczość druku w kolorze	1200x1200 dpi
Szybkość drukowania mono	10 stron A4/min
Szybkość drukowania w kolorze	7 stron A4/min
Wydruk bez marginesów	TAK
Czas do wydruku pierwszej strony	do 14 sekund
Skanowanie w kolorze	TAK
Optyczna rozdzielczość skanowania	600x600 dpi
Skanowanie do plików w formacie	BMP,JPG,PDF,PNG,RTF,PDF (przeszukiwalny),TXT,TIFF
Rozdzielczość kopiowania	600x600 dpi
Szybkość kopiowania monochromatycznego	do 8 kopii/min (ISO)



Szybkość kopiowania w kolorze	do 4 kopii/min (ISO)
Zakres skalowania	min 25 % max 400 %
Maksymalna gramatura papieru	do 300 g/m ²
Pojemność podajnika głównego	do 50 arkuszy
Automatyczny podajnik dokumentów (ADF)	TAK
Standardowe języki drukarki	PCL 3 GUI
Standardowe rozwiązania komunikacyjne	USB (2.0), USB Host (2.0), Wireless, Wi-Fi Direct, BLE
Waga produktu	ok. 2,96 kg
Zasilanie	sieciowe AC (200-240V), bateryjne – bateria w zestawie
Wymagania systemowe	Windows, Windows 10, 8.1, 8, 7: procesor 32-bitowy lub 64-bitowy, Mac OS, OS X v10.11 El Capitan, OS X v10.10 Yosemite, OS X v10.9 Mavericks, UNIX, Linux
Gwarancja	36 miesięcy

3.3.4. Modernizacja sieci LAN w budynku Urzędu Miasta i Gminy

Modernizacja sieci LAN polegać będzie na dostosowaniu lub wymianie istniejącej infrastruktury 100MB do 1000MB oraz wykonanie schematu całej infrastruktury.

3.3.5. Wdrożenie w Urzędzie Gminy usług w ramach Krajowego Węzła Identyfikacji Elektronicznej

Wykonanie wszystkich niezbędnych czynności związanych z przyłączeniem platformy e-usług dla interesantów Urzędu Gminy do Krajowego Węzła Identyfikacji Elektronicznej.

3.3.6. UPS do serwerowni

Parametr	Minimalne wymagania
Moc wyjściowa	1000VA / 900W
Topologia (zasada działania)	on-line
Czas przełączania	0
Konfiguracja faz we/wy	1/1
Stabilność napięcia wyjściowego	± 1% (praca z baterii)



Kształt napięcia wyjściowego przy pracy z baterii	Czysta sinusoida
Sprawność	89 % AC/AC, 85% tryb bat.
Akumulatory wewnętrzne	3×7,2Ah /12 V typu VRLA
Typ gniazd wyjściowych	8x IEC320 C13 / 2 sekcje po cztery gniazda
Komunikacja	Port RS 232 lub USB oraz Intelligent Slot
Oprogramowanie	Power Master Plus
Gwarancja	36 miesięcy

3.3.7. Switche zarządzalne (firewall, systemy IDS, IPS)

Parametr	Minimalne wymagania
Ilość	3 szt.
Przeznaczenie	do szaf RACK 19
Typ	Zarządzalny
Gwarancja	5 lat w serwisie sprzedawcy
Liczba portów LAN 10/100/1000	24 szt.
Porty PoE	24 szt.
Sloty SFP 1000 Mb/s	4 szt.
Obsługiwane protokoły	IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3az, IEEE 802.3i, IEEE 802.3u, IEEE 802.3x flow control, IEEE 802.3z
Rozmiar tablicy adresów MAC	8000
Prędkość magistrali wew.	56 Gb/s
Szybkość przekierowań pakietów	41.7 mpps
Obsługa VLANów	TAK
Gwarancja	36 miesięcy

3.3.8. Program do Backupu

1. Oprogramowanie musi wspierać co najmniej systemy operacyjne:	1) Windows XP i nowsze. 2) Windows Server 2003 i nowsze. 3) Windows SBS 2011/2008, 2003/2003R2. 4) Windows Storage Server 2012/2012R2, 2008R2/2008/2003.
---	---



	5) Windows MultiPoint Server 2012/2011/2010. 6) Linux
2. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:	1) Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www. 2) Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego). 3) Zarządzanie procesem tworzenia kopii zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT. 4) Definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem). 5) Zdalna instalacja agentów kopii zapasowych na maszynach z systemem operacyjnym Windows. 6) Zdalne uaktualniania agentów kopii zapasowych. 7) Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych
3. Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:	1) Kopie zapasowe całych dysków i partycji. 2) Kopie zapasowe wybranych plików i folderów. 3) Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory). 4) Zapis kopii zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczany przez producenta systemu kopii zapasowych. 5) Zapis kopii zapasowych na udziały sieciowe. 6) Zapis kopii zapasowych na serwer SFTP. 7) Zapis kopii zapasowych na dedykowaną ukrytą partycję na



	maszynie, której kopia zapasowa jest wykonywana. 8) Wyszukiwanie plików w kopiach zapasowych. 9) Szyfrowanie plików kopi zapasowych. 10) Wsparcie dla technologii VSS. 11) Kompresja plików kopi zapasowych. 12) Replikacja kopi zapasowych na kolejny nośnik (dysk, magazyn chmurowy).
4. Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:	1) Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore. 2) Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową. 3) Odtworzenie całej maszyny wirtualnej. 4) Odtworzenie poszczególnych plików i folderów. 5) Granularne odtwarzanie baz danych Microsoft Exchange. 6) Granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange. 7) Wyszukiwanie i podgląd odtwarzanych wiadomości email. 8) Granularne odtwarzanie baz danych Microsoft SQL. 9) Granularne odtwarzanie witryn i plików Microsoft SharePoint. 10) Odtwarzanie kontrolerów domeny Microsoft Active Directory.
5. Dodatkowe wymagania związane ochroną danych:	Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń.
6. Wymagania co do modelu licencjonowania rozwiązania:	1) Możliwa subskrypcja 2 letnia 2) Model licencjonowania oparty na maszynach fizycznych i hostach –



(brak limitów na chronioną ilość danych i aplikacji).

3.3.9. Rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS)

OBSŁUGA SIECI
1. 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)
2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 5. 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. 6. 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, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). 12. Konfiguracja UTM: – instalacja urządzenia w siedzibie Zamawiającego, – wdrożenie polityk zabezpieczeń zgodnie z potrzebami urzędu.
INTRUSION PREVENTION SYSTEM (IPS)
12. 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.

13. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
14. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
15. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
16. 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.
17. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
18. 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.
19. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
20. 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).

KSZTAŁTOWANIE PASMA (Traffic Shapping)

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

OCHRONA ANTYWIRUSOWA

25. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
26. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
27. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
28. 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 ANTYPSPAM

29. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
30. Ochrona antyspam ma działać w oparciu o:
- 1) białe/czarne listy,
 - 2) DNS RBL,
 - 3) Skaner heurystyczny.
31. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
32. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

33. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
34. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
- 1) PPTP VPN,
 - 2) IPSec VPN,
 - 3) SSL VPN.
35. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
36. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
37. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
38. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
39. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

40. Urządzenie ma posiadać wbudowany filtr URL.
41. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
42. Administrator ma mieć możliwość dodawania własnych kategorii URL.
43. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
- 1) blokowanie dostępu do adresu URL,
 - 2) zezwolenie na dostęp do adresu URL,
 - 3) blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
44. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
45. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.



46. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
47. 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.

UWIERZYTELNIANIE

48. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
- 1) lokalną bazę użytkowników (wewnętrzny LDAP),
 - 2) zewnętrzną bazę użytkowników (zewnętrzny LDAP),
 - 3) usługę katalogową Microsoft Active Directory.
49. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
50. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
- 1) SSL,
 - 2) Radius,
 - 3) Kerberos.
51. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
52. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
53. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

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

ROUTING (TRASOWANIE)

61. Urządzenie ma umożliwiać statyczne trasowanie pakietów.



- 62. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
- 63. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
- 64. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

ADMINISTRACJA URZĄDZENIEM

- 65. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
- 66. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
- 67. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
- 68. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
- 69. Urządzenie ma umożliwiać zarządzania z poziomu konsoli (SSH)
- 70. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
- 71. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
- 72. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
- 73. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
- 74. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
 - 1) manualnego eksportu do pliku w dowolnym momencie czasu,
 - 2) automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
- 75. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
- 76. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

RAPORTOWANIE

- 77. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
- 78. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
- 79. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.



80. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
81. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
82. W ramach posiadanej licencji urządzenie ma umożliwiać skorzystanie z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
83. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
84. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

85. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
86. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
87. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
88. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci w zakresie określenia bramy, serwerów DNS, nazwy domeny.
89. Urządzenie ma posiadać usługę DNS Proxy.
90. 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.

GWARANCJA I SERWIS

91. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
92. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

PARAMETRY SPRZĘTOWE

93. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
94. Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów.
95. Liczba portów Ethernet 10/100/1000Mbps – min.8.
96. Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
97. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
98. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2.4Gbps.
99. Przepustowość filtrowania Antywirusowego – minimum 495Mbps.
100. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 600Mbps.
101. Maksymalna liczba tuneli VPN IPSec – minimum 100.



102. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 20.
103. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
104. Obsługa interfejsów 802.11q (VLAN) – minimum 128
105. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 18 000 nowych sesji/sekundę.
106. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
107. Urządzenie nie ma limitu na liczbę użytkowników.
108. Liczba reguł filtrowania – minimum 8 192.
109. Liczba tras statycznego routingu – minimum 512.
110. Liczba tras dynamicznego routingu – minimum 10 000.

3.3.10. Urządzenie sieciowe NAS

Parametr	Minimalne wymagania
Urządzenie sieciowe typu NAS RACK	
Obsługiwane rozmiary dysków pamięci	2.5,3.5", druga generacja szeregowej magistrali komputerowej (serial ATA II), Serial ATA III
Usługa RAID	TAK, 0,1,5,6,10,JBOD
Ilość obsługiwanych rozmiarów dysków	min 8
Obsługiwane systemy plików	BTRFS,FAT,HFS+,NTFS,exFAT,ext3,ext4
Zatoka hot-swap	TAK
Model procesora: min:	AMD Ryzen V1500B 2,2 GHz
Pamięć wewnętrzna	min 4GB DDR4 ECC możliwość rozbudowy do 32 GB
Sieć	ilość portów min 4 x 1000 Mbit/s
Funkcja Wake-On-LAN	TAK
Obsługa iSCSI	TAK
Online RAID expansion	TAK
Online RAID migration	TAK
Obsługiwane protokoły sieciowe	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN
Porty	USB 3.2 min 2 szt., eSATA min 1 szt. , PCI Express x8 (Gen 3.x) min 1 szt.
Obudowa	RACK 2U
Rodzaj chłodzenia	aktywny
Zamek zatoki dysku	TAK
Diody LED	HDD, Zasilanie, Status
Zainstalowany system operacyjny	DiskStation Manager
Zasilanie: wbudowany zasilacz	2 x 250 W



Gwarancja	36 miesięcy
Dyski 8TB	
Ilość	3 szt.
Rozmiar HDD	3.5"
Pojemność HDD	8000 GB
Szybkość HDD	7200 RPM
Rozmiar bufora dysku pamięci	256 MB
Szybkość transmisji interfejsu HDD	6 Gbit/s
MTBF (Średni okres międzyawaryjny)	1200000 h
Konfiguracja NAS	– instalacja urządzenia w siedzibie zamawiającego, – konfiguracja urządzenia do robienia backupu danych wraz z oprogramowaniem do wykonywania obrazów serwera.
Gwarancja	36 miesięcy

3.3.11. Dodatkowe urządzenie sieciowe NAS

Parametr	Minimalne wymagania
Urządzenie sieciowe typu NAS	
Obsługiwane rozmiary nośników	2 x 2,5"/3,5" max 32TB
Obsługa RAID	0, 1, BASIC, JBOD
Interfejsy	USB 3.0 -2 szt, RJ-45 10/100/1000 (LAN)-1 szt., DC-in (wejście zasilania)-1 szt.
Procesor	Realtek RTD1296 (4 rdzenie, 1.4 GHz)
Pamięć RAM	512 MB
Protokoły sieciowe	AFP, iSCSI, Serwer FTP, NFS, Serwer VPN, SNMP, SSH, Telnet, WebDAV
Funkcja Wake on LAN/WAN	TAK
Licencja	na 2 kamery IP
Szyfrowanie woluminów	TAK
Gwarancja	36 miesięcy
Dyski 4TB	
Ilość	2 szt.
Rozmiar HDD	3.5"
Pojemność HDD	4000 GB



Szybkość HDD	5900 RPM
Rozmiar bufora dysku pamięci	64 MB
Szybkość transmisji interfejsu HDD	6 Gbit/s
MTBF (Średni okres międzyawaryjny)	1000000 h
Konfiguracja NAS	– instalacja urządzenia w siedzibie zamawiającego, – konfiguracja urządzenia do robienia backupu danych wraz z oprogramowaniem do wykonywania obrazów serwera.
Gwarancja	36 miesięcy

3.3.12. Wspólny Słownik Zamówień CPV:

30200000-1 Urządzenia komputerowe

30213100-6 Komputery przenośne

42962000-7 Urządzenia drukujące i graficzne

48000000-8 Pakiety i programowania i systemy informatyczne

3.3.13. Rozwiązania równoważne

W przypadku użycia w zapytaniu ofertowym, szczegółowym opisie przedmiotu zamówienia lub załącznikach odniesień do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, zamawiający dopuszcza rozwiązania równoważne opisywanym. W przypadku, gdy w opisie przedmiotu zamówienia lub załącznikach zostały użyte znaki towarowe, oznacza to, że są podane przykładowo i określają jedynie minimalne oczekiwane parametry jakościowe oraz wymagany standard. Wykonawca może zastosować materiały lub urządzenia równoważne, lecz o parametrach technicznych i jakościowych podobnych lub lepszych, których zastosowanie w żaden sposób nie wpłynie negatywnie na prawidłowe funkcjonowanie programów komputerowych, wyposażenia i sprzętu Wykonawcy, który zastosuje urządzenia lub materiały równoważne będzie obowiązany wykazać w trakcie realizacji zamówienia, że zastosowane przez niego urządzenia i materiały spełniają wymagania określone przez zamawiającego.

W przypadku, gdy wykonawca z przyczyn od niego niezależnych nie może uzyskać określonego przez zamawiającego oznakowania lub oznakowania potwierdzającego, że dane dostawy lub usługi spełniają równoważne wymagania, zamawiający w terminie przez siebie wyznaczonym akceptuje inne odpowiednie środki dowodowe, w szczególności dokumentację techniczną producenta, o ile dany wykonawca udowodni, że dostawy lub usługi, które mają zostać przez niego wykonane, spełniają wymagania określonego oznakowania lub określone wymagania wskazane przez zamawiającego.

Użycie w zapytaniu lub załącznikach wymogu posiadania certyfikatu wydanego przez jednostkę oceniającą zgodność lub sprawozdania z badań przeprowadzonych przez tę jednostkę jako środka dowodowego potwierdzającego zgodność z wymaganiami lub cechami określonymi w opisie przedmiotu zamówienia,

kryteriach oceny ofert lub warunkach realizacji zamówienia oznacza, że zamawiający akceptuje również certyfikaty wydane przez inne równoważne jednostki oceniające zgodność. Zamawiający akceptuje także inne odpowiednie środki dowodowe, w szczególności dokumentację techniczną producenta, w przypadku gdy dany wykonawca nie ma ani dostępu do certyfikatów lub sprawozdań z badań, ani możliwości ich uzyskania w odpowiednim terminie, o ile ten brak dostępu nie może być przypisany danemu wykonawcy, oraz pod warunkiem że dany wykonawca udowodni, że wykonywane przez niego dostawy lub usługi spełniają wymogi lub kryteria określone w opisie przedmiotu zamówienia, kryteriach oceny ofert lub warunkach realizacji zamówienia.

3.3.14. Wykonawca zobowiązany jest do zrealizowania zamówienia na zasadach i warunkach opisanych we wzorze umowy stanowiącym załącznik nr 6A do zapytania.

3.3.15. Miejsce dostawy: Urząd Miasta i Gminy Bolimów, ul. Łowicka 9, 99-417 Bolimów.

3.4. **Część 2 zamówienia: przeprowadzenie diagnozy cyberbezpieczeństwa, przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa, wykonanie audytu KRI wraz z poprawą procedur systemów zarządzania bezpieczeństwem w Urzędzie Miasta i Gminy Bolimów:**

3.4.1. W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji, w tym przetwarzania danych osobowych, z obowiązującymi aktami prawnymi do przeprowadzenia kompleksowego audytu bezpieczeństwa informacji w zakresie ustawowych obszarów działalności podmiotu (w tym w szczególności weryfikacji struktury organizacji oraz przepływu dokumentów, analizy zewnętrznej i wewnętrznej sieci komputerowej, analizy serwerów, testów dostępu do sieci wewnętrznej i zewnętrznej, analizy stacji roboczych, analizy kopii zapasowych, analizy poczty email, analizy ogólnego bezpieczeństwa danych i mechanizmów kontroli w podmiocie) oraz opracowania dokumentacji poaudytowej - raportu z wytycznymi do doskonalenia i rekomendacjami.

3.4.2. Diagnoza cyberbezpieczeństwa w Urzędzie Miasta i Gminy Bolimów Gminy w Bolimowie musi zostać przeprowadzona zgodnie z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369 z późn. zm.) oraz Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247 ze zm.) zwane dalej Rozporządzeniem KRI, w tym opracowanie raportu zawierającego wnioski i rekomendacje oraz przeprowadzenie szkolenia pracowników Urzędu w zakresie cyfrowego bezpieczeństwa informacji.

3.4.3. Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona zgodnie z formularzem zamieszczonym w dokumentacji konkursowej projektu Cyfrowa Gmina dostępnym na stronach Centrum Projektów Polska Cyfrowa [<https://www.gov.pl/web/cppc/cyfrowa-gmina>] - **Formularz informacji**

związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa - załącznik nr 8.

- 3.4.4. Audyt musi zostać przeprowadzony przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wykaz certyfikatów wskazanych w w/w rozporządzeniu:
- 1) Certified Internal Auditor (CIA),
 - 2) Certified Information System Auditor (CISA),
 - 3) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób,
 - 4) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób,
 - 5) Certified Information Security Manager (CISM),
 - 6) Certified in Risk and Information Systems Control (CRISC),
 - 7) Certified in the Governance of Enterprise IT (CGEIT),
 - 8) Certified Information Systems Security Professional (CISSP),
 - 9) Systems Security Certified Practitioner (SSCP),
 - 10) Certified Reliability Professional,
 - 11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert
- 3.4.5. Diagnozę cyberbezpieczeństwa należy dostarczyć w wersji elektronicznej oraz w wersji papierowej.
- 3.4.6. **Załączniki do opisu diagnozy cyberbezpieczeństwa:**
- 1) Formularz_informacji_związanych_z_przeprowadzeniem_diagnozy_cyberbezpieczeństwa,
 - 2) Rozporządzenie Mini_Cyfryzacji_wykaz_certyfikatów_uprawniających_do_przeprowadzenia_audytu
- 3.4.7. Szkolenie z zakresu cyberbezpieczeństwa ma na celu podniesienie kompetencji kadry urzędniczej w obszarze zagrożeń teleinformatycznych, podniesienie poziomu bezpieczeństwa informacyjnego w urzędzie, poznanie prawidłowej reakcji na cyberataki, poznanie podstawowych zasad i dobrych praktyk wykorzystywania technologii informatycznych oraz zdobycie umiejętności wykorzystania tej wiedzy w praktyce.
- 3.4.8. Szkolenie powinno obejmować co najmniej:
- 1) omówienie poprawnych zasad związanych z cyberbezpieczeństwem w Urzędzie,

- 2) szczegółowe informacje związane z zagrożeniami w sieci takimi jak: phishing, ransomware oraz malware i omówienie sposobów przeciwdziałania oraz zabezpieczania się przed powyższymi zagrożeniami,

3.4.9. Informacje dotyczące jednostki, w której szkolenie ma być przeprowadzone.

- 1) Liczba pracowników Urzędu objętych postępowaniem –19 osób,
- 2) Ilość lokalizacji działalności organizacji-1
- 3) Działy w organizacji: Burmistrz Miasta i Gminy, Zastępca Burmistrza, Skarbnik Gminy; Sekretarz Gminy; Referat Finansowy, Referat Gospodarki, Rozwoju Gospodarczego i Promocji, USC, Samodzielne Stanowisko ds. Zarządzania Kryzysowego, Ochrony Ludzi i Spraw Obronnych, Wieloosobowe Stanowisko ds. Organizacyjnych,

3.4.10. Informacje dotyczące wymagań w zakresie przeprowadzenia szkolenia:

- 1) Jednostką czasową szkolenia jest 1 godzina szkoleniowa (1 godzina szkolenia = 45 minut).
- 2) Szkolenia będą trwały maksymalnie 8 godzin szkoleniowych w ciągu dnia.
- 3) Szkolenia będą odbywać się w dni robocze w godzinach 7.30 – 15.30.
- 4) Szkolenia będą prowadzone w języku polskim.
- 5) Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu prac, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 14 dni przed rozpoczęciem szkolenia.
- 6) Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę.
- 7) W przypadku szkoleń trwających do 3 godzin, przewiduje się jedną przerwę trwającą 15 minut. W przypadku szkoleń trwających powyżej 3 godzin, organizowane będą dwie przerwy trwające 15 minut każda. Dodatkowo, w przypadku szkoleń trwających 8 godzin zaplanowana jest przerwa trwająca 30 minut.
- 8) W ramach organizacji szkoleń Zamawiający zapewni rekrutację osób biorących udział w szkoleniach.
- 9) W ramach organizacji szkoleń Wykonawca zapewni:
 - a) materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia, harmonogram dzienny szkolenia oraz materiały merytoryczne (np. skrypty, podręczniki, zeszyty informacyjne, broszury) w formie papierowej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Ponadto, uczestnicy otrzymają materiały pisarskie, w tym zeszyty, długopisy, ołówki itp. Materiały szkoleniowe przekazywane są nieodpłatnie Uczestnikom na własność. 1 egzemplarz materiałów szkoleniowych zostanie przekazany Zamawiającemu w celach archiwalnych.,
 - b) salę szkoleniową (w przypadku jeżeli Zamawiający nie będzie mógł zorganizować własnej sali szkoleniowej), przystosowaną do prowadzenia zajęć dydaktycznych, zapewniającą warunki do przeprowadzenia



szkolenia. Sala wyposażona będzie w wystarczającą dla wszystkich uczestników szkolenia liczbę stanowisk pracy,

- c) dostęp do sieci Internet,
- d) warunki pracy uczestników i Wykonawcy w trakcie trwania szkolenia zgodne przepisami bezpieczeństwa i higieny pracy,
- e) wystarczającą liczbę własnych licencji na oprogramowanie komputerowe wykorzystywane przy realizacji szkoleń oraz sprzęt komputerowy dla każdego Uczestnika umożliwiające przeprowadzenie szkolenia,
- f) projektor multimedialny, tablice i inne artykuły niezbędne do prowadzenia szkoleń,
- g) właściwe działania promocyjne i informacyjne dotyczące szkoleń, w tym właściwe oznakowanie sal szkoleniowych, jak również oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych Uczestnikom oraz Zamawiającemu w celach archiwalnych obowiązkowymi oznaczeniami Beneficjentów Funduszy Europejskich,
- h) wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia,
- i) kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń,
- j) prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:
 - lista obecności Uczestników szkolenia (dziennie, wypełniane oddzielnie każdego dnia szkolenia),
 - lista odbioru zaświadczeń o ukończeniu szkolenia,
 - potwierdzenie przez Uczestników odbioru materiałów szkoleniowych,
 - przeprowadzenie ankiet satysfakcji po każdym szkoleniu,
 - sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.

3.4.11. Ramowy zakres szkolenia:

- 1) Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika.
- 2) Polityka bezpieczeństwa w organizacji.
- 3) Definicja incydentu bezpieczeństwa i zasady postępowania z incydemem.
- 4) Rodzaje ataków: ataki socjotechniczne, ataki komputerowe, ataki przez sieci bezprzewodowe, ataki przez pocztę e-mail (fałszywe e-maile), ataki przez strony WWW, ataki przez telefon, phishing, spoofing, spam.
- 5) Bezpieczeństwo fizyczne - urządzenia, dokumenty, „czyste biurko”.
- 6) Zabezpieczenie informatycznych nośników danych – pendrivy i pamięci zewnętrzne.
- 7) Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.

- 8) Przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych.
 - 9) Prawidłowe korzystanie z oprogramowania antywirusowego.
 - 10) Zasady aktualizacji programów i aplikacji.
 - 11) Szyfrowanie dokumentów i poczty elektronicznej.
 - 12) Polityka haseł, zarządzanie dostępem i tożsamością.
- 3.4.12. Dodatkowe wymagania:
- 1) W ramach usługi zostanie przeszkolonych 19 osób w dwóch grupach.
 - 2) Szkolenie powinno odbywać się na terenie Gminy Bolimów.
 - 3) Szkolenie powinno trwać minimum 8 godzin szkoleniowych dla 1 grupy szkoleniowej.
- 3.4.13. Wspólny Słownik Zamówień CPV:
72800000-8 Usługi audytu komputerowego i testowanie komputerów
80510000-2 Usługi szkolenia specjalnego
- 3.4.14. Wykonawca zobowiązany jest do zrealizowania zamówienia na zasadach i warunkach opisanych we wzorze umowy stanowiącym załącznik nr 6B do zapytania.
- 3.5. Przedmiot zamówienia realizowany jest w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00.
- 3.6. Zamawiający dopuszcza składania ofert częściowych. Wykonawca może złożyć ofertę na jedną lub wszystkie części zamówienia.
- 3.7. Zamawiający nie przewiduje możliwości udzielenia zamówień, o których mowa w pkt 7 lit. g podrozdziału 6.5 Wytycznych w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020.
- 3.8. Zamawiający żąda wskazania przez Wykonawcę części zamówienia, których wykonanie zamierza powierzyć Podwykonawcy i podania przez Wykonawcę firmy Podwykonawcy (o ile są mu znani na tym etapie). Zaangażowanie Podwykonawców nie zmienia zobowiązań Wykonawcy wobec Zamawiającego za należyte wykonanie zamówienia. Wykonawca będzie odpowiedzialny za działania, uchybienia i zaniedbania Podwykonawców w takim stopniu, jakby to były działania, uchybienia i zaniedbania jego pracowników.

ROZDZIAŁ 4. TERMIN REALIZACJI UMOWY.

Przedmiot zamówienia należy zrealizować w terminie: **40 dni od dnia podpisania umowy** (dotyczy obu części zamówienia).

ROZDZIAŁ 5. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCENY ICH SPEŁNIENIA.

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na zasadach określonych w rozdziale 6 zapytania ofertowego oraz spełniają następujące warunki:

5.1. Dysponują niezbędną wiedzą i doświadczeniem:

Wykonawca spełni warunek jeżeli wykaże, że:

- 1) dla części 1 zamówienia: w ostatnich 3 latach przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał co najmniej 1 dostawę sprzętu komputerowego tj.: serwera z oprogramowaniem i urządzenia sieciowego NAS o łącznej wartości nie mniejszej niż 45 000,00 zł,
Opis sposobu oceny spełnienia warunku: weryfikacja spełnienia warunku nastąpi w oparciu o wykaz dostaw wraz z załączonymi do niego referencjami bądź innymi dokumentami potwierdzającymi należyte wykonanie, wystawionymi przez podmiot, na rzecz którego dostawy były wykonywane, wg wzoru załącznika nr 4 do zapytania ofertowego.

- 2) dla części 2 zamówienia: w ostatnich 3 latach przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał co najmniej 3 audyty bezpieczeństwa na rzecz sektora administracji publicznej.

Opis sposobu oceny spełnienia warunku: weryfikacja spełnienia warunku nastąpi w oparciu o wykaz zrealizowanych usług wraz z załączonymi do niego referencjami bądź innymi dokumentami potwierdzającymi należyte wykonanie, wystawionymi przez podmiot, na rzecz którego usługi były wykonywane, wg wzoru załącznika nr 5 do zapytania ofertowego.

- 5.2. Opis sposobu dokonywania oceny spełniania warunków udziału w postępowaniu: weryfikacja nastąpi na podstawie złożonego przez Wykonawcę oświadczenia o spełnieniu warunków udziału w postępowaniu wg wzoru stanowiącego załącznika nr 6 do zapytania ofertowego. Ocena spełniania przedstawionych powyżej warunków zostanie dokonana wg formuły: „spełnia – nie spełnia”.

- 5.3. Wykonawca, który nie spełni któregośkolwiek z warunków zostanie wykluczony z postępowania.

ROZDZIAŁ 6. PRZESŁANKI WYKLUCZENIA

- 6.1. Z postępowania o udzielenie zamówienia Zamawiający wykluczy Wykonawcę:

- 6.1.1. który jest powiązany z Zamawiającym osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przeprowadzeniem procedury wyboru Wykonawcy a Wykonawcą, polegające w szczególności na:

- 1) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
- 2) posiadaniu co najmniej 10% udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa lub nie został określony przez Instytucję Zarządzającą programem operacyjnym,

- 3) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
 - 4) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.
- 6.1.2. w stosunku do którego zachodzi którakolwiek z okoliczności wskazanych w art. 7 ust 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowe (Dz. U. z 2022 r. poz. 835), tj.:
- 1) Wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3,
 - 2) Wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3,
 - 3) Wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106) jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3.
- 6.2. Wykluczenie, o którym mowa w pkt 6.1.2. zapytania następuje na okres trwania okoliczności określonych w pkt 6.1.2. zapytania.
- 6.3. Opis sposobu dokonywania oceny spełniania warunków udziału w postępowaniu: weryfikacja nastąpi na podstawie złożonego przez Wykonawcę oświadczenia o braku podstaw wykluczenia wg wzoru stanowiącego załącznika nr 3 do zapytania ofertowego. Ocena spełniania przedstawionych powyżej warunków zostanie dokonana wg formuły: „spełnia – nie spełnia”.

ROZDZIAŁ 7. WYKAZ OŚWIADCZEŃ I DOKUMENTÓW, POTWIERDZAJĄCYCH SPEŁNIANIE WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ BRAK PODSTAW DO WYKLUCZENIA.

- 7.1. Do oferty Wykonawca zobowiązany jest dołączyć aktualne na dzień składania ofert:
- 1) oświadczenie o spełnianiu warunków udziału w postępowaniu wg wzoru stanowiącego załącznika nr 2 do zapytania ofertowego,

- 2) oświadczenie o braku podstaw wykluczenia według wzoru załącznika nr 3 do zapytania ofertowego.
- 7.2. Wykonawca składa wraz z ofertą, o ile dotyczy:
- 1) w przypadku, gdy Wykonawcę reprezentuje pełnomocnik, do oferty musi być załączone pełnomocnictwo określające jego zakres i podpisane przez osoby uprawnione do reprezentacji Wykonawcy. Pełnomocnictwo należy załączyć w formie oryginału lub kopii poświadczonej za zgodność z oryginałem przez notariusza lub radcę prawnego/adwokata lub Wykonawcę,
 - 2) pełnomocnictwo dla pełnomocnika do reprezentowania w postępowaniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia – dotyczy ofert składanych przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia. Pełnomocnik może być ustanowiony do reprezentowania Wykonawców w postępowaniu albo do reprezentowania w postępowaniu i zawarcia umowy. Pełnomocnictwo musi być złożone w formie oryginału lub kopii poświadczonej za zgodność z oryginałem przez notariusza lub radcę prawnego/adwokata lub Wykonawcę.
- 7.3. Zamawiający przed udzieleniem zamówienia, najpierw dokona oceny ofert w oparciu o kryteria oceny ofert określone w rozdziale 13 zapytania ofertowego, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu. W tym celu Zamawiający wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 5 dni, terminie aktualnych na dzień złożenia dokumentów.
- 7.4. Na wezwanie Zamawiającego, o którym mowa w pkt 7.3. zapytania, Wykonawca zobowiązany jest złożyć następujące dokumenty w celu potwierdzenia spełnienia warunków udziału w postępowaniu:
- 1) dla części 1 zamówienia: wykaz zrealizowanych dostaw wraz z załączonymi do niego referencjami bądź innymi dokumentami potwierdzającymi należyte wykonanie, wystawionymi przez podmiot, na rzecz którego usługi były wykonywane według wzoru stanowiącego załącznika nr 4 do zapytania ofertowego,
 - 2) dla części 2 zamówienia: wykaz zrealizowanych usług wraz z załączonymi do niego referencjami bądź innymi dokumentami potwierdzającymi należyte wykonanie, wystawionymi przez podmiot, na rzecz którego usługi były wykonywane według wzoru stanowiącego załącznika nr 4 do zapytania ofertowego.
- 7.5. Dokumenty sporządzone w języku obcym muszą być złożone wraz z tłumaczeniami na język polski.
- 7.6. Zamawiający zastrzega możliwość sprawdzenia informacji zawartych w powyższych dokumentach.

ROZDZIAŁ 8. INFORMACJA DLA WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA

- 8.1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w

sprawie zamówienia publicznego. Pełnomocnictwo w formie pisemnej (oryginał lub kopia potwierdzona za zgodność z oryginałem przez notariusza lub radcę prawnego/adwokata lub Wykonawcę) należy dołączyć do oferty. Wszelka korespondencja dotycząca niniejszego postępowania prowadzona będzie z pełnomocnikiem.

- 8.2. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenia, o których mowa w pkt 7.1. ppkt 2 zapytania, składa każdy z Wykonawców.
- 8.3. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia dokumenty potwierdzające spełnianie warunków udziału w postępowaniu składane są w taki sposób, aby wynikało, że łącznie są spełniane przez wszystkich Wykonawców.
- 8.4. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia dokumenty i oświadczenia składające się na ofertę powinny być podpisane przez pełnomocnika.

ROZDZIAŁ 9. INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ I DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI.

- 9.1. W niniejszym postępowaniu o udzielenie zamówienia komunikacja (wszelkie zawiadomienia, oświadczenia, wnioski oraz informacje) między Zamawiającym a Wykonawcami odbywają się za pośrednictwem operatora pocztowego w rozumieniu ustawy z dnia 2 listopada 2012 r. – Prawo pocztowe (t.j. Dz. U. z 2018 r. poz. 2188 z późn. zm.), osobiście, za pośrednictwem postańca lub przy użyciu środków komunikacji elektronicznej za pomocą poczty elektronicznej na adres mail: ug.sekretariat@bolimow.pl lub przy użyciu systemu dostępnego na Bazie Konkurencyjności: <https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl/>.
- 9.2. Wszelkie zawiadomienia, oświadczenia, wnioski oraz informacje przekazane w formie elektronicznej wymagają na żądanie każdej ze stron, niezwłocznego potwierdzenia faktu ich otrzymania.
- 9.3. W przypadku braku potwierdzenia otrzymania korespondencji przez Wykonawcę, Zamawiający domniema, że korespondencja wysłana przez Zamawiającego na adres email, podany przez Wykonawcę, została mu doręczona w sposób umożliwiający zapoznanie się z jej treścią.
- 9.4. W korespondencji związanej z niniejszym postępowaniem Wykonawcy powinni posługiwać się znakiem postępowania: **GRP.7011.67.2022**.
- 9.5. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści zapytania ofertowego.
- 9.6. Pytania co do przedmiotu zamówienia składa się pod rygorem nieważności w postaci elektronicznej za pomocą poczty elektronicznej na adres mail: ug.sekretariat@bolimow.pl lub poprzez system dostępny na stronie: <https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl/>. Szczegółowy tryb składania oferty opisuje podręcznik dostępny pod adresem: <https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl/pomoc>.
- 9.7. Zamawiający udzieli wyjaśnień niezwłocznie, jeżeli prośba o udzielenie wyjaśnień wpłynęła nie później, niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. Jeżeli prośba taka wpłynęła w terminie późniejszym albo prośba ta dotyczy

udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień, albo pozostawić wniosek bez rozpoznania.

- 9.8. Treści odpowiedzi wraz z wyjaśnieniami zostaną opublikowane w na stronie <https://bip.ugbolimow.nv.pl> w zakładce Zapytania ofertowe, w w przypadku pytań zadanych za pomocą Bazy Konkurencyjności również w tej bazie.
- 9.9. Zamawiający zastrzega sobie prawo do nieudzielenia odpowiedzi na pytania przekazane mu w sposób i terminie innym niż opisane w pkt 9.6. i 9.7 zapytania.
- 9.10. Zamawiający nie udziela żadnych ustnych i telefonicznych informacji, wyjaśnień czy odpowiedzi na kierowane do Zamawiającego zapytania.
- 9.11. Osoby uprawnione przez Zamawiającego do porozumiewania się z Wykonawcami:
 - 1) Katarzyna Choińska tel. 46 819 50 81,
 - 2) Wioletta Grebelska tel. 46 819 50 80.
- 9.12. Zamawiający nie przewiduje zorganizowania zebrania z Wykonawcami.

ROZDZIAŁ 10. OPIS SPOSOBU PRZYGOTOWYWANIA OFERTY.

- 10.1. Wykonawca może złożyć jedną ofertę dla danej części zamówienia. Złożenie więcej niż jednej oferty na daną część spowoduje odrzucenie wszystkich ofert złożonych przez Wykonawcę w danej części postępowania.
- 10.2. Zamawiający nie dopuszcza możliwości składania ofert wariantowych. Złożenie więcej niż jednej oferty na daną część spowoduje odrzucenie wszystkich ofert złożonych przez Wykonawcę w danej części postępowaniu.
- 10.3. Oferta musi być sporządzona z zachowaniem formy pisemnej lub postaci elektronicznej pod rygorem nieważności.
- 10.4. Treść oferty musi być zgodna z treścią zapytania ofertowego.
- 10.5. Oferta wraz z załącznikami oraz wszystkie dokumenty złożone przez Wykonawcę muszą być sporządzone w języku polskim. Każdy dokument składający się na ofertę lub złożony wraz z ofertą sporządzony w języku innym niż polski musi być złożony wraz z tłumaczeniem na język polski.
- 10.6. Oferta musi być podpisana przez Wykonawcę, tj. osobę (osoby) reprezentującą Wykonawcę, zgodnie z zasadami reprezentacji wskazanymi we właściwym rejestrze lub osobę (osoby) upoważnioną do reprezentowania Wykonawcy.
- 10.7. Jeżeli osoba (osoby) podpisująca ofertę (reprezentująca Wykonawcę lub Wykonawców występujących wspólnie) działa na podstawie pełnomocnictwa, pełnomocnictwo to w formie oryginału lub kopii poświadczonej za zgodność z oryginałem przez notariusza lub radcę prawnego/adwokata lub Wykonawcę musi zostać dołączone do oferty.
- 10.8. Poprawki lub zmiany w ofercie, powinny być parafowane własnoręcznie przez osobę podpisującą ofertę.
- 10.9. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.
- 10.10. **Oferta musi zawierać:**
 - 1) formularz ofertowy sporządzony z wykorzystaniem wzoru stanowiącego **załącznik nr 1** do zapytania ofertowego,
 - 2) w przypadku, gdy Wykonawcę reprezentuje pełnomocnik, do oferty musi być załączone pełnomocnictwo określające jego zakres i podpisane przez osoby uprawnione do reprezentacji Wykonawcy. Pełnomocnictwo należy załączyć w

- formie oryginału lub kopii poświadczonej za zgodność z oryginałem przez notariusza lub radcę prawnego/adwokata lub Wykonawcę (**jeżeli dotyczy**),
- 3) pełnomocnictwo do reprezentowania wszystkich Wykonawców ubiegających się o udzielenie zamówienia. Pełnomocnik może być ustanowiony do reprezentowania Wykonawców w postępowaniu albo do reprezentowania w postępowaniu i zawarcia umowy. Pełnomocnictwo musi być złożone w formie oryginału lub kopii poświadczonej za zgodność z oryginałem przez notariusza lub radcę prawnego/adwokata lub Wykonawcę (**jeżeli dotyczy**),
 - 4) oświadczenia, o których mowa w pkt 7.1. zapytania ofertowego.

ROZDZIAŁ 11. MIEJSCE, SPOSÓB ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT.

11.1. Ofertę należy złożyć:

- 1) w siedzibie Zamawiającego tj. Urzędzie Miasta i Gminy Bolimów ul. Łowicka 9, pokój nr 15 (sekretariat) w poniedziałek w godzinach od 10.00 do 18.00, wtorek-piątek w godzinach od 7.30 do 15.30 lub
- 2) za pośrednictwem Bazy Konkurencyjności:
<https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl/>. Szczegółowy tryb składania oferty opisuje podręcznik dostępny pod adresem:
<https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl/pomoc>

11.2. W przypadku składania ofert w sposób wskazany w pkt 11.1. ppkt 1 ofertę należy umieścić w opakowaniu i zabezpieczyć w sposób uniemożliwiający zapoznanie się z jej zawartością przed upływem terminu składania ofert. Opakowanie zewnętrzne nie może zawierać innych napisów i oznaczeń wskazujących na identyfikację Wykonawcy lub jego uprawnionego przedstawiciela. Na opakowaniu zewnętrznym należy zamieścić adres Zamawiającego: Gmina Bolimów, 99-417 Bolimów ul. Łowicka 9 oraz napis „**Oferta na dostawę sprzętu komputerowego i oprogramowania w ramach projektu grantowego „Cyfrowa Gmina”**”. **Nie otwierać przed dniem 12 lipca 2022 roku do godz. 10.30**”. Na opakowaniu wewnętrznym należy zamieścić: nazwę i dokładny adres Wykonawcy oraz napis „**Oferta na dostawę sprzętu komputerowego i oprogramowania w ramach projektu grantowego „Cyfrowa Gmina”**”.

11.3. W przypadku składania ofert w sposób wskazany w pkt 11.1. ppkt 2 ofertę należy złożyć w formie skanów lub w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym. Oferta składana w formie skanów musi być opatrzona własnoręcznym podpisem osoby upoważnionej do reprezentowania Wykonawcy zgodnie z formą reprezentacji Wykonawcy, a następnie zeskanowana i w takiej formie złożona w Bazie Konkurencyjności. Podpis musi być czytelny, pozwalający na identyfikację osoby podpisującej ofertę. W takim przypadku Zamawiający zastrzega sobie prawo do żądania przesłania oryginału oferty.

11.4. Termin składania ofert **upływa w dniu 12 lipca 2022 roku o godz. 10.00.**

11.5. Oferty przesłane przez operatora pocztowego będą zakwalifikowane do rozpatrzenia pod warunkiem dostarczenia ich przez operatora pocztowego do Urzędu Miasta i Gminy Bolimów **do dnia 12 lipca 2022 roku do godz. 10.00.**

11.6. Za datę złożenia oferty w sposób wskazany w pkt 11.1. ppkt 2 uważa się datę widoczną w systemie Baza Konkurencyjności.

- 11.7. Oferty złożone w innej formie niż wskazana w pkt 11.1. zapytania, złożone po terminie nie będą rozpatrywane.
- 11.8. Zamawiający nie ponosi odpowiedzialności za:
- 1) złożenie przez Wykonawcę oferty po terminie składania ofert,
 - 2) złożenie oferty w innym miejscu lub w inny sposób niż określonym w pkt 11.1 zapytania ofertowego,
 - 3) złożenie oferty nieopisanej w sposób określony w pkt 11.2. zapytania ofertowego uniemożliwiający identyfikację postępowania, którego dotyczy.
- 11.9. Otwarcie ofert nastąpi w dniu **12 lipca 2022 roku o godz. 10.30**.
- 11.10. Wykonawca, przed upływem terminu do składania ofert, może zmienić lub wycofać ofertę.
- 11.11. W przypadku złożenia oferty w sposób wskazany w pkt 11.1. ppkt 1 zapytania wprowadzone zmiany muszą być złożone według takich samych zasad, jak składana oferta tj. w opakowaniu oznaczonym jak w pkt 11.2. z dodatkowym napisem „ZMIANA”. Opakowania oznaczone „ZMIANA” zostaną otwarte przy otwarciu oferty Wykonawcy, który wprowadził zmiany i po stwierdzeniu poprawności procedury dokonywania zmian, zostaną dołączone do oferty.
- 11.12. W przypadku wycofania oferty złożonej w sposób wskazany w pkt 11.1. ppkt 1 Wykonawca składa pisemne powiadomienie według takich samych zasad jak wprowadzenie zmian w ofercie w opakowaniu oznaczonym jak w pkt 11.2. z dodatkowym napisem „WYCOFANIE”. Opakowanie oznaczone „WYCOFANIE” będzie otwarte w pierwszej kolejności. Opakowanie z ofertą, której dotyczy wycofanie nie będzie otwierane.
- 11.13. W przypadku złożenia oferty w sposób wskazany w pkt 11.1. ppkt 2 zapytania zmianę lub wycofanie oferty należy dokonać zgodnie z instrukcją opublikowaną na stronie: <https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl/pomoc>.
- 11.14. Po upływie terminu do składania ofert Wykonawca nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.
- 11.15. Niezwłocznie po otwarciu ofert Zamawiający zamieści na własnej stronie internetowej <https://bip.ugbolimow.nv.pl> oraz na stronie <https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl/> informacje dotyczące:
- 1) firm oraz adresów Wykonawców, którzy złożyli oferty w terminie,
 - 2) ceny brutto złożonych ofert.
- 11.16. Dokumenty, o których mowa w pkt 7.4. zapytania, Wykonawca złoży w formie pisemnej lub w formie elektronicznej. Dokumenty w formie pisemnej należy złożyć w siedzibie Zamawiającego, tj. Urzędzie Miasta i Gminy Bolimów, 99-417 Bolimów ul. Łowicka 9. Dokumenty w formie elektronicznej (opatrzone kwalifikowanym podpisem elektronicznym) należy przesłać za pomocą poczty elektronicznej na adres mail: ug.sekretariat@bolimow.pl.

ROZDZIAŁ 12. OPIS SPOSOBU OBLICZENIA CENY.

- 12.1. Dopuszcza się składanie ofert częściowych. Wykonawca w formularzu ofertowym, stanowiącym załącznik nr 1 do zapytania ofertowego, poda cenę brutto, wartość podatku VAT i cenę netto, **oddzielnie dla każdej części zamówienia**.

- 12.2. Cena będzie podana w PLN i stanowić będzie wynagrodzenie ryczałtowe.
- 12.3. Cenę należy podać z dokładnością do dwóch miejsc po przecinku.
- 12.4. Cena ofertowa winna uwzględniać wszystkie wymagania niniejszego zapytania ofertowego oraz obejmować wszystkie koszty, jakie poniesie Wykonawca z tytułu zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia.
- 12.5. Do porównania i oceny ofert Zamawiający przyjmie całkowitą cenę brutto zamówienia, jaką poniesie na realizację przedmiotu zamówienia.
- 12.6. Rozliczenia pomiędzy Wykonawcą a Zamawiającym będą dokonywane w PLN.

ROZDZIAŁ 13. OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT.

- 13.1. Zamawiający przy wyborze oferty będzie kierował się następującymi kryteriami i ich znaczeniem:

Kryterium	Waga	Maksymalna liczba punktów, jakie może otrzymać oferta za dane kryterium
Cena (C)	100%	100 pkt

- 13.2. Punkty za kryterium „Cena” (C) zostaną obliczone według wzoru:

$$P_i(C) = \frac{C_{\min}}{C_i} \times 100$$

gdzie:

$P_i(C)$ – oznacza liczbę punktów, jakie otrzyma badana oferta „i” za kryterium „Cena (C)”;

$C_{\min}$ – najniższa cena ofertowa brutto spośród wszystkich ocenianych ofert;

C_i – cena brutto oferty badanej „i”.

Przy obliczaniu punktów, Zamawiający zastosuje zaokrąglenie do dwóch miejsc po przecinku według zasady, że trzecia cyfra po przecinku od 5 w górę powoduje zaokrąglenie drugiej cyfry po przecinku w górę o 1. Jeśli trzecia cyfra po przecinku jest mniejsza niż 5, to druga cyfra po przecinku nie ulega zmianie.

- 13.3. Zamawiający wybierze ofertę, która uzyska największą liczbę punktów.

ROZDZIAŁ 14. OCENA I WYBÓR OFERTY.

- 14.1. Zamawiający odrzuci ofertę, jeżeli:
 - 1) jej treść nie odpowiada treści i wymaganiom określonym w niniejszym zapytaniu ofertowym,
 - 2) jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji;
 - 3) została złożona przez Wykonawcę wykluczonego z udziału w postępowaniu,

- 4) Wykonawca nie zgodził się na poprawienie omyłki, o której mowa w pkt. 14.2. ppkt 3 zapytania ofertowego.
 - 5) Wykonawca nie wyraził zgody na przedłużenie terminu związania ofertą, o której mowa w pkt 17.4 zapytania,
 - 6) jest nieważna na podstawie odrębnych przepisów.
- 14.2. Zamawiający poprawi w treści oferty:
- 1) oczywiste omyłki pisarskie,
 - 2) oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
 - 3) inne omyłki polegające na niezgodności oferty z dokumentami zapytania ofertowego, niepowodujące istotnych zmian w treści oferty,
- niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.
- 14.3. W przypadku, o którym mowa w pkt 14.2 ppkt 3 Zamawiający wyznacza Wykonawcy odpowiedni termin na wyrażenie zgody na poprawienie w ofercie omyłki lub zakwestionowanie jej poprawienia. Brak odpowiedzi w wyznaczonym terminie uznaje się za wyrażenie zgody na poprawienie omyłki.
- 14.4. Zamawiający może wezwać Wykonawcę do wyjaśnienia treści złożonej oferty, w tym dotyczących dokumentów złożonych na potwierdzenie spełnienia warunków udziału w postępowaniu, jednak wyjaśnienia nie mogą prowadzić do negocjacji lub zmiany treści oferty.
- 14.5. W toku badania i oceny ofert Zamawiający może wezwać Wykonawcę do złożenia, uzupełnienia lub poprawienia zawierających błędy oświadczeń i dokumentów.
- 14.6. Zamawiający zastrzega sobie prawo sprawdzania w toku oceny oferty wiarygodności przedstawionych przez Wykonawców dokumentów, oświadczeń, wykazów, danych i informacji.
- 14.7. Jeżeli nie będzie można dokonać wyboru oferty najkorzystniejszej ze względu na to, że zostały złożone oferty o takiej samej cenie, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych.
- 14.8. Wykonawcy, składając oferty dodatkowe, nie mogą zaoferować cen wyższych niż zaoferowane w złożonych ofertach.
- 14.9. Wykonawcy, którzy złożą oferty zostaną zawiadomieni o wynikach postępowania w formie elektronicznej na adres e-mail wskazany w ofercie. Informacja o wynikach postępowania zostanie również opublikowana na stronie internetowej:
<https://bip.ugbolimow.nv.pl> oraz na stronie
<https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl/>

ROZDZIAŁ 15. ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI ZAWIERANEJ UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO ORAZ WARUNKI ISTOTNE ZMIANY UMOWY.

- 15.1. Po przeprowadzeniu postępowania Zamawiający podpisze z Wykonawcą umowę, której istotne postanowienia zawarto we wzorze stanowiącym załącznik nr 6A lub 6B do zapytania ofertowego.

- 15.2. Wykonawca akceptuje treść wzoru umowy na wykonanie przedmiotu zamówienia zgodnie z oświadczeniem zawartym w treści formularza ofertowego.
- 15.3. Zamawiający przewiduje możliwość dokonania zmiany postanowień umowy w następującym zakresie:
- 15.3.1. Część 1 zamówienia:
- 1) zmiany będącej wynikiem zmiany umowy o dofinansowanie projektu zawartej pomiędzy Zamawiającym a Instytucją Zarządzającą w zakresie terminów (w tym terminu rzeczowej realizacji projektu) lub wysokości i warunków płatności dofinansowania realizacji projektu stanowiącego przedmiot niniejszej umowy,
 - 2) zmiany terminu realizacji przedmiotu umowy w przypadku:
 - a) siły wyższej - rozumianej jako wystąpienie zdarzenia nadzwyczajnego, zewnętrznego, niemożliwego do przewidzenia i zapobieżenia, którego nie dało się uniknąć nawet przy zachowaniu najwyższej staranności, a które uniemożliwia Wykonawcy wykonanie przedmiotu umowy. W razie wystąpienia siły wyższej Strony umowy zobowiązane są dołożyć wszelkich starań w celu ograniczenia do minimum opóźnienia w wykonywaniu swoich zobowiązań umownych, powstałych na skutek działania siły wyższej. (Pod pojęciem siły wyższej rozumie się w szczególności zdarzenia i okoliczności takie jak: klęska żywiołowa, działania wojenne, rebelie, terroryzm, rewolucja, powstanie, inwazja, bunt, zamieszki, strajk spowodowany przez inne osoby - nie związane z realizacją inwestycji, itp.),
 - b) zmiany parametrów technicznych przedmiotu zamówienia w przypadku, gdy z przyczyn technicznych (w szczególności zakończenia produkcji lub niedostępności na rynku parametru/komponentu zaoferowanego w ofercie) konieczne jest dokonanie zmiany np. rodzaju/modelu/typu, a parametry te będą nie gorsze niż parametry zaproponowane w ofercie, z zastrzeżeniem, że zmiana nie może wpłynąć na termin wykonania zamówienia i na wynagrodzenie Wykonawcy. W przypadku zaistnienia konieczności dokonania zmian, Wykonawca zobowiązany jest wystąpić do Zamawiającego z pisemnym wnioskiem o wyrażenie zgody na wprowadzenie zmian oraz pisemnie uzasadnić potrzebę ich wprowadzenia. Wszystkie zmiany muszą być zaakceptowane przez Zamawiającego pisemnie,
 - c) okoliczności leżących po stronie Zamawiającego i nie wynikających z przyczyn leżących po stronie Wykonawcy (np. wstrzymanie, zawieszenie, przerwa w realizacji),
 - d) wystąpienia okoliczności, których strony umowy nie były w stanie przewidzieć, pomimo zachowania należytej staranności ,
 - 3) zmiany, rezygnacji, bądź wprowadzenia Podwykonawcy w trakcie realizacji przedmiotu umowy,
 - 4) zmiany powszechnie obowiązujących przepisów prawa mających wpływ na treść złożonej oferty w takim zakresie w jakim będzie to niezbędne w celu dostosowania postanowień umowy do zaistniałego stanu prawnego,
 - 5) zastąpienia Wykonawcy, któremu Zamawiający udzielił zamówienia, nowym wykonawcą w wyniku połączenia, podziału, upadłości, restrukturyzacji lub nabycia dotychczasowego Wykonawcy lub jego przedsiębiorstwa, o ile nowy wykonawca spełnia warunki udziału w postępowaniu i nie zachodzą wobec niego podstawy wykluczenia wskazane w zapytaniu ofertowym oraz nie pociąga to za sobą innych

istotnych zmian umowy. Przekształcony Wykonawca musi nadal spełniać warunki udziału w postępowaniu oraz nie mogą zachodzić wobec niego podstawy wykluczenia wskazane w zapytaniu ofertowym,

- 6) zmiany wynagrodzenia Wykonawcy, w przypadku:
 - a) zmiany stawki podatku od towarów i usług. W takim przypadku Wykonawca ma obowiązek w terminie 30 dni od zmiany wysokości stawki podatku od towarów i usług złożyć do Zamawiającego pisemny wniosek. W przypadku zmiany podatku od towarów i usług wartość wynagrodzenia netto nie zmieni się, a wartość wynagrodzenia brutto zostanie wyliczona na podstawie nowych przepisów,
- 7) zmiany sposobu rozliczenia umowy lub dokonywania płatności na rzecz Wykonawcy na skutek zmian zawartej przez Zamawiającego umowy o dofinansowanie projektu lub wytycznych dotyczących realizacji projektu

15.3.2. Część 2 zamówienia:

- 8) zmiany będącej wynikiem zmiany umowy o dofinansowanie projektu zawartej pomiędzy Zamawiającym a Instytucją Zarządzającą w zakresie terminów (w tym terminu rzeczowej realizacji projektu) lub wysokości i warunków płatności dofinansowania realizacji projektu stanowiącego przedmiot niniejszej umowy,
- 9) zmiany terminu realizacji przedmiotu umowy w przypadku:
 - e) siły wyższej - rozumianej jako wystąpienie zdarzenia nadzwyczajnego, zewnętrznego, niemożliwego do przewidzenia i zapobieżenia, którego nie dało się uniknąć nawet przy zachowaniu najwyższej staranności, a które uniemożliwia Wykonawcy wykonanie przedmiotu umowy. W razie wystąpienia siły wyższej Strony umowy zobowiązane są dołożyć wszelkich starań w celu ograniczenia do minimum opóźnienia w wykonywaniu swoich zobowiązań umownych, powstałych na skutek działania siły wyższej. (Pod pojęciem siły wyższej rozumie się w szczególności zdarzenia i okoliczności takie jak: klęska żywiołowa, działania wojenne, rebelie, terroryzm, rewolucja, powstanie, inwazja, bunt, zamieszki, strajk spowodowany przez inne osoby - nie związane z realizacją inwestycji, itp.),
 - f) okoliczności leżących po stronie Zamawiającego i nie wynikających z przyczyn leżących po stronie Wykonawcy (np. wstrzymanie, zawieszenie, przerwa w realizacji),
 - g) wystąpienia okoliczności, których strony umowy nie były w stanie przewidzieć, pomimo zachowania należytej staranności ,
- 10) zmiany, rezygnacji, bądź wprowadzenia Podwykonawcy w trakcie realizacji przedmiotu umowy,
- 11) zmiany powszechnie obowiązujących przepisów prawa mających wpływ na treść złożonej oferty w takim zakresie w jakim będzie to niezbędne w celu dostosowania postanowień umowy do zaistniałego stanu prawnego,
- 12) zastąpienia Wykonawcy, któremu Zamawiający udzielił zamówienia, nowym wykonawcą w wyniku połączenia, podziału, upadłości, restrukturyzacji lub nabycia dotychczasowego Wykonawcy lub jego przedsiębiorstwa, o ile nowy wykonawca spełnia warunki udziału w postępowaniu i nie zachodzą wobec niego podstawy wykluczenia wskazane w zapytaniu ofertowym oraz nie pociągają to za sobą innych istotnych zmian umowy. Przekształcony Wykonawca musi nadal spełniać warunki

udziału w postępowaniu oraz nie mogą zachodzić wobec niego podstawy wykluczenia wskazane w zapytaniu ofertowym,

13) zmiany wynagrodzenia Wykonawcy, w przypadku:

b) zmiany stawki podatku od towarów i usług. W takim przypadku Wykonawca ma obowiązek w terminie 30 dni od zmiany wysokości stawki podatku od towarów i usług złożyć do Zamawiającego pisemny wniosek. W przypadku zmiany podatku od towarów i usług wartość wynagrodzenia netto nie zmieni się, a wartość wynagrodzenia brutto zostanie wyliczona na podstawie nowych przepisów,

14) zmiany sposobu rozliczenia umowy lub dokonywania płatności na rzecz Wykonawcy na skutek zmian zawartej przez Zamawiającego umowy o dofinansowanie projektu lub wytycznych dotyczących realizacji projektu.

15.4. Zmiana postanowień umowy, z zastrzeżeniem przypadków określonych w pkt 15.5. może nastąpić wyłącznie za zgodą obu Stron umowy, wyrażoną w drodze aneksu do umowy pod rygorem nieważności.

15.5. Zmianie podlegają także wszystkie nieistotne postanowienia w stosunku do treści oferty, a także inne nieistotne zmiany, które nie stanowią zmiany umowy i nie jest wymagane zawarcie aneksu do umowy, w tym między innymi

- 1) zmiana przedstawicieli stron umowy odpowiedzialnych za jej realizację,
- 2) zmiana danych związana z obsługą administracyjno-organizacyjną umowy, zmiana danych teleadresowych Wykonawcy lub Zamawiającego - zmiana ta następuje poprzez pisemne zgłoszenie tego faktu drugiej Stronie i nie wymaga zawarcia aneksu do umowy.

ROZDZIAŁ 16. UNIEWAŻNIENIE POSTĘPOWANIA.

Zamawiający zastrzega sobie prawo unieważnienia postępowania na każdym etapie bez podania przyczyny.

ROZDZIAŁ 17. POZOSTAŁE INFORMACJE.

17.1. Zamawiający zastrzega sobie możliwość zmiany lub uzupełnienia treści zapytania ofertowego, przed upływem terminu na składanie ofert. Informacja o wprowadzeniu zmiany lub uzupełnieniu treści zapytania ofertowego zostanie opublikowana w miejscach publikacji zapytania.

17.2. Jeżeli wprowadzone zmiany lub uzupełnienia treści zapytania ofertowego będą wymagały zmiany treści ofert, Zamawiający przedłuży termin składania ofert o czas potrzebny na dokonanie zmian w ofercie.

17.3. Termin związania ofertą wynosi 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

17.4. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą, z tym, że Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 30 dni.

17.5. Odmowa wyrażenia zgody, o której mowa w pkt 17.4., spowoduje odrzucenie oferty.

- 17.6. Podpisanie umowy nastąpi w siedzibie Zamawiającego. O terminie i godzinie podpisania umowy Zamawiający powiadomi Wykonawcę.
- 17.7. W przypadku, gdy wybrany Wykonawca odstąpi od podpisania umowy z Zamawiającym, możliwe jest podpisanie umowy z kolejnym Wykonawcą, który w postępowaniu o udzielenie zamówienia uzyskał kolejną najwyższą liczbę punktów.

ROZDZIAŁ 18. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH W PROGRAMIE CYFROWA POLSKA 2014-2020 (POPC 2014-2020).

Zasady przetwarzania danych osobowych w programie Polska Cyfrowa 2014-2020 (POPC 2014-2020). Ze względu na to, że to Minister Funduszy i Polityki Regionalnej - jako Instytucja Zarządzająca POPC 2014-2020 - określa jakie dane osobowe, w jaki sposób i w jakim celu będą przetwarzane w związku z realizacją Programu, pełni on rolę administratora danych osobowych przetwarzanych w związku z realizacją POPC 2014-2020 w rozumieniu RODO [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) z dnia 27 kwietnia 2016 r. (Dz. Urz.UE. L Nr 119, ztr.1). Przy czym jest on administratorem zarówno wobec danych osobowych, które samodzielnie pozyskał, jak i wobec danych osobowych pozyskanych przez inne podmioty zaangażowane w realizację Programu (tj. przez innych administratorów, którzy w tym przypadku pełnią dodatkowo funkcję podmiotów przetwarzających dane osobowe [Podmiotami przetwarzającymi są: Instytucja Pośrednicząca POPC 2014-2020, beneficjenci oraz inne podmioty zaangażowane w realizację POPC 2014-2020, którym Minister (lub inny upoważniony podmiot) powierzył przetwarzanie danych osobowych w ramach POPC 2014-2020])). Minister Funduszy i Polityki Regionalnej jest także administratorem danych osobowych, które przetwarza jako beneficjent projektów współfinansowanych ze środków POPC 2014-2020. Minister Funduszy i Polityki Regionalnej jest również administratorem danych zgromadzonych w zarządzanym przez niego Centralnym Systemie Teleinformatycznym wspierającym realizację POPC 2014-2020.

1. Cel przetwarzania danych osobowych

Minister Funduszy i Polityki Regionalnej przetwarza dane osobowe w celu realizacji zadań przypisanych Instytucji Zarządzającej POPC 2014-2020, w zakresie, w jakim jest to niezbędne dla realizacji tego celu. Minister Funduszy i Polityki Regionalnej przetwarza dane osobowe w szczególności w celach:

- 1) udzielania wsparcia beneficjentom ubiegającym się o dofinansowanie i realizującym projekty,
- 2) potwierdzania kwalifikowalności wydatków,
- 3) wnioskowania o płatności do Komisji Europejskiej,
- 4) raportowania o nieprawidłowościach,
- 5) ewaluacji,
- 6) monitoringu,
- 7) kontroli,
- 8) audytu,

- 9) sprawozdawczości,
- 10) działań informacyjno-promocyjnych.

2. Podstawy prawne przetwarzania

Przetwarzanie danych osobowych w związku z realizacją POPC 2014-2020 odbywa się zgodnie z RODO. Podstawą prawną przetwarzania danych jest konieczność realizacji obowiązków spoczywających na Ministrze Funduszy i Polityki Regionalnej - jako na Instytucji Zarządzającej – na podstawie przepisów prawa europejskiego i krajowego (art. 6 ust. 1 lit. c RODO).

Obowiązki te wynikają m.in. z przepisów ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020 oraz przepisów prawa europejskiego:

- 1) rozporządzenia Parlamentu Europejskiego i Rady nr 1303/2013 z dnia 17 grudnia 2013 r. ustanawiające go wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego, oraz ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego oraz uchylającego Rozporządzenie Rady (WE) nr 1083/2006, 2),
- 2) rozporządzenia wykonawczego Komisji (UE) nr 1011/2014 z dnia 22 września 2014 r. ustanawiającego szczegółowe przepisy wykonawcze do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 w odniesieniu do wzorów służących do przekazywania Komisji określonych informacji oraz szczegółowe przepisy dotyczące wymiany informacji między beneficjentami a instytucjami zarządzającymi, certyfikującymi, audytowymi i pośredniczącymi.

3. Podstawą przetwarzania danych osobowych przez Ministra są również:

- 1) konieczność realizacji umowy, której stroną jest osoba, której dane dotyczą (art. 6 ust. 1 lit. B RODO) - podstawa ta ma zastosowanie m. in. do danych osobowych osób prowadzących samodzielną działalność gospodarczą, z którymi Minister zawarł umowy w celu realizacji POPC 2014-2020,
- 2) wykonywanie zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Ministrowi (art. 6 ust. 1 lit e RODO) - podstawa ta ma zastosowanie m. in. Do organizowanych przez Ministra konkursów i akcji promocyjnych dotyczących Programu,
- 3) uzasadniony interes prawny Ministra Funduszy i Polityki Regionalnej (art. 6 ust. 1 lit f RODO) –podstawa ta ma zastosowanie m.in. do danych osobowych przetwarzanych w związku z realizacją umów w ramach Funduszy Europejskich. W ramach POPC 2014-2020 w działaniu 3.1 – Działania szkoleniowe na rzecz rozwoju kompetencji cyfrowych przetwarzane są dane szczególnej kategorii (dane o niepełnosprawności). Podstawą prawną przetwarzania jest wyraźna zgoda osoby, której dane dotyczą (art. 9 ust. 2 lit a RODO).

4. Rodzaje przetwarzanych danych

Minister Funduszy i Polityki Regionalnej w celu realizacji POPC 2014-2020 przetwarza dane osobowe m. in.:

- 1) pracowników, wolontariuszy, praktykantów i stażystów reprezentujących lub wykonujących zadania na rzecz podmiotów zaangażowanych w obsługę i realizację POPC 2014-2020,
- 2) osób wskazanych do kontaktu, osób upoważnionych do podejmowania wiążących decyzji oraz innych osób wykonujących zadania na rzecz wnioskodawców, beneficjentów i partnerów,
- 3) uczestników szkoleń, konkursów, konferencji, komitetów monitorujących, grup roboczych, grup sterujących oraz spotkań informacyjnych lub promocyjnych organizowanych w ramach POPC 2014-2020.

ROZDZIAŁ 19. KLAUZULA INFORMACYJNA Z ART. 13 RODO.

Zgodnie z 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 04.05.2016, str. 1), dalej „RODO”, informuję, że:

- administratorem Pani/Pana danych osobowych jest Burmistrz Miasta i Gminy Bolimów, 99-417 Bolimów ul. Łowicka 9;
- administrator wyznaczył inspektora ochrony danych, z którym może się Pani/Pan skontaktować poprzez email s.koziel@4consult.com.pl z inspektorem ochrony danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych
- Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym postępowaniem o udzielenie zamówienia publicznego;
- odbiorcami Pani/Pana danych osobowych będą odbiorcy upoważnieni z mocy prawa w celu przeprowadzenia i kontroli niniejszego postępowania oraz osoby lub podmioty, biorcy udział w postępowaniu, którym udostępniona zostanie dokumentacja postępowania na ich wniosek, a także osoby i podmioty upoważnione zgodnie z obowiązującymi przepisami prawa i zapisami zawartymi w niniejszym zapytaniu ofertowym,
- Pani/Pana dane osobowe będą przechowywane przez czas, określony przepisami prawa, związanymi z realizacją przedmiotu niniejszej umowy oraz w celach archiwizacyjnych, a po tym czasie zostaną zniszczone albo zwrócone drugiej stronie umowy;
- obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego na realizację zamówienia objętego niniejszym zapytaniem ofertowym;
- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- posiada Pani/Pan:

- na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
- na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych;
- 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;
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- 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**
-

ROZDZIAŁ 20. WYKAZ ZAŁĄCZNIKÓW.

Załącznikami do niniejszego zapytania ofertowego są następujące dokumenty:

- 1) Załącznik nr 1 – wzór formularza oferty,
- 2) Załącznik nr 2 – oświadczenie o spełnianiu warunków udziału w postępowaniu,
- 3) Załącznik nr 3 – wzór oświadczenia o braku podstaw wykluczenia,
- 4) Załącznik nr 4 – wzór wykazu dostaw,
- 5) Załącznik nr 5 – wzór wykazu zrealizowanych usług,
- 6) Załącznik nr 6A - wzór umowy dla części 1,
- 7) Załącznik nr 6A - wzór umowy dla części 2.