



MIASTO I GMINA BIERUTÓW

ul. Moniuszki 12
tel. 71/314 62 51
fax. 71/314 64 32
e-mail: bierutow@bierutow.pl

56-420 Bierutów

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA (FAKULTATYWNE NEGOCJACJE)

ZAMAWIAJĄCY: MIASTO I GMINA BIERUTÓW

Zaprasza do złożenia oferty w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym z fakultatywnymi negocjacjami o wartości zamówienia nie przekraczającej progów unijnych o jakich stanowi art. 3 ustawy z 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 ze zm.) – dalej pzp. na dostawy pn.

Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”

Przedmiotowe postępowanie prowadzone jest przy użyciu środków komunikacji elektronicznej. Składanie ofert następuje za pośrednictwem platformy zakupowej dostępnej pod adresem internetowym: https://platformazakupowa.pl/pn/um_bierutow

Nr postępowania: IR.2710.15.2022.JP

Bierutów, dnia 05.07.2022 r.

ZATWIERDZAM:

SPIS TREŚCI

ROZDZIAŁ I. NAZWA I ADRES ZAMAWIAJĄCEGO.....	5
ROZDZIAŁ II. ADRES STRONY INTERNETOWEJ, NA KTÓREJ UDOSTĘPNIANE BĘDĄ ZMIANY I WYJAŚNIENIA TREŚCI SWZ ORAZ INNE DOKUMENTY ZAMÓWIENIA BEZPOŚREDNIO ZWIĄZANE Z POSTĘPOWANIEM O UDZIELENIE ZAMÓWIENIA.....	5
ROZDZIAŁ III. TRYB UDZIELENIE ZAMÓWIENIA	5
ROZDZIAŁ IV. PROWADZENIE PROCEDURY WRAZ Z NEGOCJACJAMI.....	5
ROZDZIAŁ V. OPIS PRZEDMIOTU ZAMÓWIENIA.....	6
ROZDZIAŁ VI. OPIS CZĘŚCI ZAMÓWIENIA, JEŻELI ZAMAWIAJĄCY DOPUSZCZA SKŁADANIE OFERT CZĘŚCIOWYCH.....	9
ROZDZIAŁ VII. INFORMACJE DOTYCZĄCE OFERT WARIANTOWYCH, W TYM INFORMACJE O SPOSOBIE PRZEDSTAWIANIA OFERT WARIANTOWYCH ORAZ MINIMALNE WARUNKI, JAKIM MUSZĄ ODPOWIADAĆ OFERTY WARIANTOWE, JEŻELI ZAMAWIAJĄCY WYMAGA LUB DOPUSZCZA ICH SKŁADANIE.....	9
ROZDZIAŁ VIII. INFORMACJA O OBOWIĄZKU OSOBISTEGO WYKONANIA PRZEZ WYKONAWCĘ KLUCZOWYCH CZĘŚCI ZAMÓWIENIA, JEŻELI ZAMAWIAJĄCY DOKONUJE TAKIEGO ZASTRZEŻENIA ZGODNIE Z ART. 121 USTAWY PZP	9
ROZDZIAŁ IX. INFORMACJA DLA WYKONAWCÓW POLEGAJĄCYCH NA ZASOBACH INNYCH PODMIOTÓW, NA ZASADACH OKREŚLONYCH W ART. 118 USTAWY PZP ORAZ ZAMIERZAJĄCYCH POWIERZYĆ WYKONANIE CZĘŚCI ZAMÓWIENIA PODWYKONAWCOM	10
ROZDZIAŁ X. INFORMACJA DLA WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA (SPÓŁKI CYWILNE/ KONSORCJA).....	11
ROZDZIAŁ XI. WYKONAWCA MAJĄCY SIEDZIBĘ LUB MIEJSCE ZAMIESZKANIA POZA TERYTERIUM RZECZYPOSPOLITEJ POLSKIEJ	12
ROZDZIAŁ XII. WALUTA, W JAKIEJ BĘDĄ PROWADZONE ROZLICZENIA ZWIĄZANE Z REALIZACJĄ NINIEJSZEGO ZAMÓWIENIA PUBLICZNEGO	12
ROZDZIAŁ XIII. TERMIN WYKONANIA ZAMÓWIENIA	12
ROZDZIAŁ XIV. WARUNKI UDZIAŁU W POSTĘPOWANIU.....	12
ROZDZIAŁ XV. PODSTAWY WYKLUCZENIA	12

ROZDZIAŁ XVI. WYKAZ PODMIOTOWYCH I PRZEDMIOTOWYCH ŚRODKÓW DOWODOWYCH ORAZ INNYCH DOKUMENTÓW LUB OŚWIADCZEŃ, JAKICH MOŻE ŻĄDAĆ ZAMAWIAJĄCY OD WYKONAWCY	13
ROZDZIAŁ XVII . UDZIELANIE WYJAŚNIEŃ TREŚCI SWZ	17
ROZDZIAŁ XVIII. INFORMACJE O ŚRODKACH KOMUNIKACJI ELEKTRONICZNEJ, PRZY UŻYCIU KTÓRYCH ZAMAWIAJĄCY BĘDZIE KOMUNIKOWAŁ SIĘ Z WYKONAWCAMI, ORAZ INFORMACJE O WYMAGANIACH TECHNICZNYCH I ORGANIZACYJNYCH SPORZĄDZANIA, WYSYŁANIA I ODBIERANIA KORESPONDENCJI ELEKTRONICZNEJ	17
ROZDZIAŁ XIX. WSKAZANIE OSÓB UPRAWNIONYCH DO KOMUNIKOWANIA SIĘ Z WYKONAWCAMI	20
ROZDZIAŁ XX. OMYŁKI W OFERCIE.....	21
ROZDZIAŁ XXI. WYMAGANIA DOTYCZĄCE WADIUM	21
ROZDZIAŁ XXII. TERMIN ZWIĄZANIA OFERTĄ.....	21
ROZDZIAŁ XXIII. OPIS SPOSOBU PRZYGOTOWANIA OFERT	22
ROZDZIAŁ XXIV. SPOSÓB ORAZ TERMIN SKŁADANIA OFERT	24
ROZDZIAŁ XXV. TERMIN OTWARCIA OFERT	25
ROZDZIAŁ XXVI. SPOSÓB OBLICZENIA CENY.....	25
ROZDZIAŁ XXVII. OPIS KRYTERIÓW OCENY OFERT, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW, I SPOSOBU OCENY OFERT	26
ROZDZIAŁ XXVIII. WYBÓR NAJKORZYSTNIEJSZEJ OFERTY	27
ROZDZIAŁ XXIX. INFORMACJE O FORMALNOŚCIACH, JAKIE MUSZĄ ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO	27
ROZDZIAŁ XXX. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY	28
ROZDZIAŁ XXXI. INFORMACJE O TREŚCI ZAWIERANEJ UMOWY ORAZ MOŻLIWOŚCI JEJ ZMIANY	28
ROZDZIAŁ XXXII. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY	28
ROZDZIAŁ XXXIII. ZAŁĄCZNIKI DO SWZ	29
Załącznik Nr 1 – do SWZ Formularz ofertowy	30

Załącznik Nr 2 – do SWZ_Oświadczenie wykonawcy	97
Załącznik Nr 3 – do SWZ_Oświadczenie podmiotu udostępniającego zasoby	101
Załącznik Nr 4a – do SWZ_Opis przedmiotu zamówienia – część nr 1	104
Załącznik Nr 4b – do SWZ_Opis przedmiotu zamówienia – część nr 2	111
Załącznik Nr 4c – do SWZ_Opis przedmiotu zamówienia – część nr 3.....	118
Załącznik Nr 4d – do SWZ_Opis przedmiotu zamówienia – część nr 4	123
Załącznik Nr 4e – do SWZ_Opis przedmiotu zamówienia – część nr 5	125
Załącznik Nr 4f – do SWZ_Opis przedmiotu zamówienia – część nr 6	133
Załącznik Nr 4g – do SWZ_Opis przedmiotu zamówienia – część nr 7	145
Załącznik Nr 5 – do SWZ_Projekt umowy	162
Załącznik Nr 6 do SIWZ - Wzór umowy o powierzenie przetwarzania danych osobowych	183
Załącznik Nr 7 do SWZ – ZOBOWIĄZANIE INNEGO PODMIOTU	189
Załącznik Nr 8 do SWZ – Oświadczenie o grupie kapitałowej.....	191
Załącznik Nr 9 do SWZ – Klauzula informacyjna.....	193

ROZDZIAŁ I. NAZWA I ADRES ZAMAWIAJĄCEGO

Nazwa oraz adres Zamawiającego: Miasto i Gmina Bierutów, ul. Moniuszki 12, 56-420 Bierutów

Numer tel.: 71 314 62 51

Adres poczty elektronicznej: bierutow@bierutow.pl

Adres strony internetowej prowadzonego postępowania: <https://bierutow.biuletyn.net/>

Adres profilu nabywcy: https://platformazakupowa.pl/pn/um_bierutow (dedykowana platforma zakupowa do obsługi komunikacji w formie elektronicznej pomiędzy Zamawiającym a Wykonawcami oraz składania ofert).

ROZDZIAŁ II. ADRES STRONY INTERNETOWEJ, NA KTÓREJ UDOSTĘPNIANE BĘDĄ ZMIANY I WYJAŚNIENIA TREŚCI SWZ ORAZ INNE DOKUMENTY ZAMÓWIENIA BEZPOŚREDNIO ZWIĄZANE Z POSTĘPOWANIEM O UDZIELENIE ZAMÓWIENIA

Zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia będą udostępniane na stronie internetowej: <https://bierutow.biuletyn.net/> na profilu nabywcy: https://platformazakupowa.pl/pn/um_bierutow.

ROZDZIAŁ III. TRYB UDZIELENIE ZAMÓWIENIA

1. Niniejsze postępowanie prowadzone jest w trybie podstawowym o jakim stanowi art. 275 pkt 2 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2021 r., poz. 1129 ze zm.) oraz niniejszej Specyfikacji Warunków Zamówienia, zwaną dalej SWZ.
2. Zamawiający przewiduje wybór najkorzystniejszej oferty z możliwością prowadzenia negocjacji.
3. Zamawiający nie przewiduje aukcji elektronicznej.
4. Zamawiający nie przewiduje złożenia oferty w postaci katalogów elektronicznych.
5. Zamawiający nie prowadzi postępowania w celu zawarcia umowy ramowej.
6. Zamawiający nie zastrzega możliwości ubiegania się o udzielenie zamówienia wyłącznie przez wykonawców, o których mowa w art. 94 pzp.

ROZDZIAŁ IV. PROWADZENIE PROCEDURY WRAZ Z NEGOCJACJAMI

1. Zamawiający nie korzysta z uprawnienia, o jakim stanowi art. 288 ust. 1 pzp.
2. W przypadku podjęcia decyzji o prowadzeniu negocjacji w pierwszym kroku zamawiający poinformuje równocześnie wszystkich wykonawców, którzy złożyli oferty, o wykonawcach:
 - 1) których oferty nie zostały odrzucone, oraz punktacji przyznanej ofertom w każdym

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

- kryterium oceny ofert i łącznej punktacji,
- 2) których oferty zostały odrzucone,
- podając uzasadnienie faktyczne i prawne.
 3. Zamawiający w zaproszeniu do negocjacji wskaże miejsce, termin i sposób prowadzenia negocjacji oraz kryteria oceny ofert, w ramach których będą prowadzone negocjacje w celu ulepszenia treści ofert.
 4. Prowadzone negocjacje mają poufny charakter. Żadna ze stron nie może, bez zgody drugiej strony, ujawniać informacji technicznych i handlowych związanych z negocjacjami. Zgoda jest udzielana w odniesieniu do konkretnych informacji i przed ich ujawnieniem.
 5. Po zakończeniu negocjacji z wszystkimi wykonawcami, zamawiający informuje o tym fakcie uczestników negocjacji oraz zaprasza ich do składania ofert dodatkowych.
 6. Zaproszenie do złożenia ofert dodatkowych będzie zawierać co najmniej:
 - 1) nazwę oraz adres zamawiającego, numer telefonu, adres poczty elektronicznej oraz strony internetowej prowadzonego postępowania,
 - 2) sposób i termin składania ofert dodatkowych oraz język lub języki, w jakich muszą one być sporządzone, oraz termin otwarcia tych ofert.
 7. Wykonawca może złożyć ofertę dodatkową, która zawiera nowe propozycje w zakresie treści oferty podlegających ocenie w ramach kryteriów oceny ofert wskazanych przez zamawiającego w zaproszeniu do negocjacji.
 8. Oferta dodatkowa nie może być mniej korzystna w żadnym z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji niż oferta złożona w odpowiedzi na ogłoszenie o zamówieniu.
 9. Oferta przestaje wiązać wykonawcę w zakresie, w jakim złoży on ofertę dodatkową zawierającą korzystniejsze propozycje w ramach każdego z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji.
 10. Oferta dodatkowa, która jest mniej korzystna w którymkolwiek z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji niż oferta złożona w odpowiedzi na ogłoszenie o zamówieniu, podlega odrzuceniu.

ROZDZIAŁ V. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest realizacja zadania pn. **Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”** z podziałem na następujące części:
W ramach działania cyfryzacji biur, jednostek publicznych, jednostek podległych i nadzorowanych:
Część nr 1 – Zakup serwerów;
Część nr 2 – Modernizacja wewnętrznej sieci LAN;

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

Część nr 3 – Zakup urządzenia wielofunkcyjnego z możliwością skanowania do sieci;

Część nr 4 – Zakup oprogramowania biurowego;

Część nr 5 – Zakup systemu do tworzenia kopii bezpieczeństwa;

W ramach działania zapewnienie cyberbezpieczeństwa samorządowych systemów informatycznych :

Część nr 6 – Zakup oprogramowania do monitorowania urządzeń sieciowych;

Część nr 7 – Zakup oprogramowania i urządzenia do ochrony brzegu sieci.

2. Na realizację przedmiotowego zamówienia Zamawiający otrzymał grant na podstawie umowy o powierzenie grantu nr 2944/1/2021 z dnia 10.02.2022r. 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, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00.

3. Przedmiot zamówienia obejmuje dostawę sprzętu i oprogramowania do siedziby Urzędu Miejskiego w Bierutowie:

W ramach działania cyfryzacji biur, jednostek publicznych, jednostek podległych i nadzorowanych:

Część nr 1 – zakup serwerów: serwery szt. 2 dla Urzędu Miejskiego w Bierutowie – zakup 2 serwerów w celu przystosowania do wymagań systemu umożliwiającego realizację zdalnej obsługi mieszkańców (dla urzędu),

Część nr 2 – modernizacja wewnętrznej sieci LAN: modernizacja szkieletu sieci LAN w celu dostosowania do obowiązujących standardów, podniesienia poziomu bezpieczeństwa usług oraz przystosowanie do świadczenia zdalnych usług dla mieszkańców (w urzędzie),

Część nr 3 – zakup urządzenia wielofunkcyjnego z możliwością skanowania do sieci: sieciowe urządzenie wielofunkcyjne szt. 1 – urządzenie niezbędne do digitalizacji dokumentów w celu usprawnienia pracy zdalnej (dla urzędu),

Część nr 4 – zakup oprogramowania biurowego: oprogramowanie Microsoft 365 (zakup licencji na 18 miesięcy) – 90 licencji dla urzędu i jednostek podległych,

Część nr 5 – zakup systemu do tworzenia kopii bezpieczeństwa: system do backupu szt. 1 – zapewnienie ciągłości działania systemów informatycznych dla urzędu,

W ramach działania zapewnienie cyberbezpieczeństwa samorządowych systemów informatycznych:

Część nr 6 – zakup oprogramowania do monitorowania urządzeń sieciowych:

specjalistyczne oprogramowanie do ochrony danych i inwentaryzacji zasobów sieciowych (dla urzędu),

Część nr 7 – zakup oprogramowania i urządzenia do ochrony brzegu sieci:

specjalistyczne oprogramowanie i urządzenie do ochrony brzegu sieci dla urzędu.

4. Szczegółowy opis przedmiotu zamówienia zawarty jest w Specyfikacjach technicznych stanowiących załączniki nr 4a-4g do SWZ odpowiednio dla danej części. Specyfikacja techniczna zawiera minimalne wymagania, które musi spełniać oferowany przedmiot zamówienia.
5. Wykonawca zobowiązuje się do prawidłowego wykonania przedmiotu zamówienia, zgodnie z wymaganiami określonymi w Specyfikacji Warunków Zamówienia i postanowieniami projektu umowy oraz zasadami wiedzy technicznej, zasadami należytej staranności oraz obowiązującymi normami i przepisami.
6. Adres dostawy przedmiotu zamówienia: ul. Moniuszki 12, 56-420 Bierutów.
7. O terminie dostawy Wykonawca zobowiązany jest zawiadomić Zamawiającego co najmniej z 2-dniowym wyprzedzeniem. Dostawa przedmiotu umowy nastąpi w godzinach 8:00-14:00.
8. Wykonawca zobowiązuje się dostarczyć przedmiot Zamówienia na własny koszt i ryzyko do miejsca wskazanego przez Zamawiającego.
9. Wykonawca musi zagwarantować możliwość ewentualnych napraw dostarczonego sprzętu. Dane teleadresowe punktu serwisowego Wykonawca wskaże w protokole odbioru dostarczonego sprzętu.
10. Wykonawca zobowiązuje się do dostarczenia sprzętu fabrycznie nowego, nieużywanego, wolnego od wad fizycznych i prawnych oraz wydania dokumentacji dotyczącej dostarczonego przedmiotu zamówienia np. certyfikatów, atestów, deklaracji zgodności, instrukcji obsługi itp.
11. Odbiór zadania nastąpi w formie protokołu, po uprzednim stwierdzeniu jego zgodności z warunkami zamówienia.
12. Oznaczenie wg wspólnego słownika CPV:
CPV 32420000 - Urządzenia sieciowe
CPV 48310000 - Pakiety oprogramowania do tworzenia dokumentów
CPV 48820000 - Serwery
CPV 48730000 - Pakiety oprogramowania zabezpieczającego
CPV 48710000 - Pakiety oprogramowania do kopii zapasowych i odzyskiwania
CPV 32428000 – Modernizacja sieci

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

UWAGA: Zadanie dofinansowane 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 dotyczące realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00.

ROZDZIAŁ VI. OPIS CZĘŚCI ZAMÓWIENIA, JEŻELI ZAMAWIAJĄCY DOPUSZCZA SKŁADANIE OFERT CZĘŚCIOWYCH

1. Zamówienie zostało podzielone na wyodrębnione części:
W ramach działania cyfryzacji biur, jednostek publicznych, jednostek podległych i nadzorowanych:
Część nr 1 – Zakup serwerów;
Część nr 2 – Modernizacja wewnętrznej sieci LAN;
Część nr 3 – Zakup urządzenia wielofunkcyjnego z możliwością skanowania do sieci;
Część nr 4 – Zakup oprogramowania biurowego;
Część nr 5 – Zakup systemu do tworzenia kopii bezpieczeństwa;
W ramach działania zapewnienie cyberbezpieczeństwa samorządowych systemów informatycznych:
Część nr 6 – Zakup oprogramowania do monitorowania urządzeń sieciowych;
Część nr 7 – Zakup oprogramowania i urządzenia do ochrony brzegu sieci.
2. Zamawiający **dopuszcza** składanie ofert częściowych – oddzielnie dla każdej części zamówienia.
3. Wykonawca może złożyć ofertę na jedną lub więcej części. Ocenie będzie podlegać oddzielnie każda część zamówienia.

ROZDZIAŁ VII. INFORMACJE DOTYCZĄCE OFERT WARIANTOWYCH, W TYM INFORMACJE O SPOSOBIE PRZEDSTAWIANIA OFERT WARIANTOWYCH ORAZ MINIMALNE WARUNKI, JAKIM MUSZĄ ODPOWIADAĆ OFERTY WARIANTOWE, JEŻELI ZAMAWIAJĄCY WYMAGA LUB DOPUSZCZA ICH SKŁADANIE

Zamawiający nie dopuszcza składania ofert wariantowych.

ROZDZIAŁ VIII. INFORMACJA O OBOWIĄZKU OSOBISTEGO WYKONANIA PRZEZ WYKONAWCĘ KLUCZOWYCH CZĘŚCI ZAMÓWIENIA, JEŻELI ZAMAWIAJĄCY DOKONUJE TAKIEGO ZASTRZEŻENIA ZGODNIE Z ART. 121 USTAWY PZP

1. Zamawiający nie dokonuje zastrzeżenia dotyczącego obowiązku osobistego wykonania przez Wykonawcę kluczowych części Zamówienia.
2. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy.

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

3. Zamawiający żąda wskazania przez wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez wykonawcę firm podwykonawców.
4. Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia.
5. Pozostałe wymagania dotyczące podwykonawstwa zostały określone we Wzorze umowy (jeśli dotyczy).

ROZDZIAŁ IX. INFORMACJA DLA WYKONAWCÓW POLEGAJĄCYCH NA ZASOBACH INNYCH PODMIOTÓW, NA ZASADACH OKREŚLONYCH W ART. 118 USTAWY PZP ORAZ ZAMIERZAJĄCYCH POWIERZYĆ WYKONANIE CZĘŚCI ZAMÓWIENIA PODWYKONAWCOM

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
2. W odniesieniu do warunków dotyczących doświadczenia, wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonują świadczenie do realizacji którego te zdolności są wymagane.
3. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów. Wzór oświadczenia stanowi załącznik nr 7 do SWZ.
4. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w ust. 3, potwierdza, że stosunek łączący wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
 - 1) zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby;
 - 2) sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
 - 3) czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje dostawy, których wskazane zdolności dotyczą.
5. Zamawiający ocenia, czy udostępniane wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe, pozwalają na wykazanie przez wykonawcę spełniania warunków udziału w postępowaniu, a także bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane

względem wykonawcy.

6. Jeżeli zdolności techniczne lub zawodowe podmiotu udostępniającego zasoby nie potwierdzają spełniania przez wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tego podmiotu podstawy wykluczenia, zamawiający żąda, aby wykonawca w terminie określonym przez zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.
7. UWAGA: Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.
8. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia, wraz z oświadczeniem, o którym mowa w Rozdziale XIV ust. 1 SWZ, także oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, w zakresie, w jakim wykonawca powołuje się na jego zasoby, zgodnie z katalogiem dokumentów określonych w Rozdziale XVI SWZ.
9. Wykonawca, który zamierza powierzyć wykonanie części zamówienia podwykonawcom, na etapie postępowania o udzielenie zamówienia publicznego jest zobowiązany wskazać w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom oraz o ile jest to wiadome, podać firmy podwykonawców.

ROZDZIAŁ X. INFORMACJA DLA WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA (SPÓŁKI CYWILNE/ KONSORCJA)

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo winno być załączone do oferty.
2. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenia, o których mowa w Rozdziale XVI ust. 1 pkt 1 SWZ, składa każdy z wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
3. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika, które prace wykonają poszczególni wykonawcy.
4. Oświadczenia i dokumenty potwierdzające brak podstaw do wykluczenia z postępowania składa każdy z Wykonawców wspólnie ubiegających się o zamówienie.

ROZDZIAŁ XI. WYKONAWCA MAJĄCY SIEDZIBĘ LUB MIEJSCE ZAMIESZKANIA POZA TERYTORIUM RZECZYPOSPOLITEJ POLSKIEJ

Wykonawca mający siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej składa dokumenty zgodnie z przepisami Rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (Dz. U. z 2020 r., poz. 2415).

ROZDZIAŁ XII. WALUTA, W JAKIEJ BĘDĄ PROWADZONE ROZLICZENIA ZWIĄZANE Z REALIZACJĄ NINIEJSZEGO ZAMÓWIENIA PUBLICZNEGO

Wszelkie rozliczenia związane z realizacją niniejszego zamówienia dokonywane będą w złotych polskich [PLN].

ROZDZIAŁ XIII. TERMIN WYKONANIA ZAMÓWIENIA

Termin realizacji zamówienia: **Część nr 1 */ Część nr 2 */ Część nr 3 */ Część nr 4 */ Część nr 5 */ Część nr 6 */ Część nr 7 *** – do 60 dni od dnia zawarcia umowy.

ROZDZIAŁ XIV. WARUNKI UDZIAŁU W POSTĘPOWANIU

Zamawiający nie określa warunków udziału w postępowaniu.

ROZDZIAŁ XV. PODSTAWY WYKLUCZENIA

1. Z postępowania o udzielenie zamówienia wyklucza się Wykonawców, w stosunku do których zachodzi którakolwiek z okoliczności, o której mowa w:
 - 1) art. 108 ust. 1 pzp;
 - 2) art. 109 ust. 1 pkt 4, 5, 7 pzp., tj.:
 - a) w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywnością zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury;
 - b) który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych dowodów;
 - c) który z przyczyn leżących po jego stronie, w znacznym stopniu lub zakresie nie wykonał lub nienależycie wykonał albo długotrwale nienależycie wykonywał istotne zobowiązanie wynikające z wcześniejszej umowy w sprawie zamówienia

publicznego lub umowy koncesji, co doprowadziło do wypowiedzenia lub odstąpienia od umowy, odszkodowania, wykonania zastępczego lub realizacji uprawnień z tytułu rękojmi za wady.

- 3) art. 7 ust. 1 Ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, (Dz. U. 2022 poz. 835), zwana dalej „UOBN”.
2. Zgodnie z art. art. 7 ust. 1 UOBN z postępowania o udzielenie zamówienia zamawiający wyklucza Wykonawcę:
 - 1) 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 UOBN;
 - 2) 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 UOBN;
 - 3) 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 UOBN.
 3. Wykluczenie, o którym mowa w ust. 2 następować będzie na okres trwania ww. okoliczności. W przypadku wykonawcy lub uczestnika konkursu wykluczonego na podstawie art. 7 ust. 1 UOBN, Zamawiający odrzuca ofertę takiego Wykonawcy.
 4. Zamawiający będzie weryfikował przesłankę wykluczenia, o której mowa w ust. 2 na podstawie:
 - 1) wykazów określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014,
 - 2) listy Ministra właściwego do spraw wewnętrznych obejmującej osoby i podmioty, wobec których są stosowane środki, o których mowa w art. 1 UOBN.

ROZDZIAŁ XVI. WYKAZ PODMIOTOWYCH I PRZEDMIOTOWYCH ŚRODKÓW DOWODOWYCH ORAZ INNYCH DOKUMENTÓW LUB OŚWIADCZEŃ, JAKICH MOŻE ŻAĆ ZAMAWIAJĄCY OD WYKONAWCY

1. Do oferty Wykonawca zobowiązany jest dołączyć:

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

- 1) aktualne na dzień składania ofert oświadczenie o spełnianiu warunków udziału w postępowaniu oraz o braku podstaw do wykluczenia z postępowania – zgodnie z załącznikiem nr 2 do SWZ,
 - 2) oświadczenie podmiotu udostępniającego zasoby uwzględniające przesłanki wykluczenia z art. 7 ust. 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego składane na podstawie art. 125 ust. 5 ustawy Pzp – zgodnie z załącznikiem nr 3 do SWZ (jeśli dotyczy),
 - 3) opis przedmiotu zamówienia – wg załącznika nr 4a-4g do SWZ,
 - 4) pełnomocnictwo do reprezentowania wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia, ewentualnie umowa o współdziałaniu, z której będzie wynikać przedmiotowe pełnomocnictwo. Pełnomocnik może być ustanowiony do reprezentowania Wykonawców w postępowaniu albo do reprezentowania w postępowaniu i zawarcia umowy. Pełnomocnictwo winno być załączone w formie oryginału lub notarialnie poświadczonej kopii,
 - 5) dokumenty, z których wynika prawo do podpisania oferty względnie do podpisania innych dokumentów składanych wraz z ofertą, chyba, że Zamawiający może je uzyskać w szczególności za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r., poz. 346) a wykonawca wskazał to wraz ze złożeniem oferty. O ile prawo do ich podpisania nie wynika z dokumentów złożonych wraz z ofertą.
2. Informacje zawarte w oświadczeniu, o którym mowa w ust. 1 pkt 1 stanowią wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.
 3. Zamawiający wzywa Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni od dnia wezwania, podmiotowych środków dowodowych, jeżeli wymagał ich złożenia w ogłoszeniu o zamówieniu lub dokumentach zamówienia, aktualnych na dzień złożenia podmiotowych środków dowodowych.
4. **Podmiotowe środki dowodowe:**
- 1) oświadczenie wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy, o braku przynależności do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16.02.2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r. poz. 275), z innym wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w

postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej -załącznik nr 8 do SWZ;

- 2) odpis lub informacja z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;
- 3) zaświadczenie właściwego naczelnika urzędu skarbowego potwierdzające, że wykonawca nie zalega z opłacaniem podatków i opłat, w zakresie art. 109 ust. 1 pkt 1 ustawy, wystawione nie wcześniej niż 3 miesiące przed jego złożeniem, a w przypadku zalegania z opłacaniem podatków lub opłat wraz z zaświadczeniem zamawiający żąda złożenia dokumentów potwierdzających, że odpowiednio przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert wykonawca dokonał płatności należnych podatków lub opłat wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
- 4) zaświadczenie albo inny dokument właściwej terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych lub właściwego oddziału regionalnego lub właściwej placówki terenowej Kasy Rolniczego Ubezpieczenia Społecznego potwierdzające, że wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne i zdrowotne, w zakresie art. 109 ust. 1 pkt 1 ustawy, wystawione nie wcześniej niż 3 miesiące przed jego złożeniem, a w przypadku zalegania z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne wraz z zaświadczeniem albo innym dokumentem zamawiający żąda złożenia dokumentów potwierdzających, że odpowiednio przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert wykonawca dokonał płatności należnych składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności.

5. **Przedmiotowe środki dowodowe:**

- 1) w celu potwierdzenia zgodności oferowanej dostawy z wymaganiami i cechami określonymi w Specyfikacji Warunków Zamówienia i opisie przedmiotu zamówienia Zamawiający żąda od Wykonawców złożenia wraz z ofertą następujących przedmiotowych środków dowodowych:
 - opis przedmiotu zamówienia złożonego w formie specyfikacji technicznej określającej parametry oferowanego przedmiotu zamówienia zgodnie z załącznikami nr 4a-4g do SWZ.
- 2) jeżeli Wykonawca nie złoży przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe będą niekompletne, Zamawiający wezwie

Wykonawcę do ich złożenia lub uzupełnienia w wyznaczonym terminie.

6. Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast zaświadczenia, o którym mowa w ust. 4 pkt 3, zaświadczenia albo innego dokumentu potwierdzającego, że wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne, o których mowa w ust. 4 pkt 4, lub odpisu albo informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, o których mowa w ust. 4 pkt 2 – składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że nie naruszył obowiązków dotyczących płatności podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne.
7. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w ust. 4 pkt 2, zastępuje się je odpowiednio w całości lub w części dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy.
8. Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych, jeżeli:
 - 1) może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile wykonawca wskazał w oświadczeniu, o którym mowa w art. 125 ust. 1 pzp dane umożliwiające dostęp do tych środków;
 - 2) podmiotowym środkiem dowodowym jest oświadczenie, którego treść odpowiada zakresowi oświadczenia, o którym mowa w art. 125 ust. 1.
9. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które zamawiający posiada, jeżeli wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.
10. W zakresie nieuregulowanym ustawą pzp lub niniejszą SWZ do oświadczeń i dokumentów składanych przez Wykonawcę w postępowaniu zastosowanie mają w szczególności przepisy rozporządzenia Ministra Rozwoju Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy oraz Rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu

sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie.

ROZDZIAŁ XVII . UDZIELANIE WYJAŚNIEŃ TREŚCI SWZ

1. Wykonawca może zwrócić się do zamawiającego z wnioskiem o wyjaśnienie treści SWZ.
2. Wykonawca może zwrócić się do zamawiającego z wnioskiem o wyjaśnienie odpowiednio treści SWZ albo opisu potrzeb i wymagań.
3. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania odpowiednio ofert albo ofert podlegających negocjacom, pod warunkiem że wniosek o wyjaśnienie treści odpowiednio SWZ albo opisu potrzeb i wymagań wpłynął do zamawiającego nie później niż na 4 dni przed upływem terminu składania odpowiednio ofert.
4. Jeżeli zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w ust. 3, przedłuży termin składania odpowiednio ofert albo ofert podlegających negocjacom o czas niezbędny do zapoznania się wszystkich zainteresowanych wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia odpowiednio ofert albo ofert podlegających negocjacom.
5. W przypadku gdy wniosek o wyjaśnienie treści SWZ albo opisu potrzeb i wymagań nie wpłynął w terminie, o którym mowa w ust. 3, zamawiający nie ma obowiązku udzielania odpowiednio wyjaśnień SWZ albo opisu potrzeb i wymagań oraz obowiązku przedłużenia terminu składania odpowiednio ofert albo ofert podlegających negocjacom.
6. Przedłużenie terminu składania ofert, o których mowa w ust. 4, nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści odpowiednio SWZ albo opisu potrzeb i wymagań.
7. Treść zapytań wraz z wyjaśnieniami zamawiający udostępnia, bez ujawniania źródła zapytania, na stronie internetowej prowadzonego postępowania.

ROZDZIAŁ XVIII. INFORMACJE O ŚRODKACH KOMUNIKACJI ELEKTRONICZNEJ, PRZY UŻYCIU KTÓRYCH ZAMAWIAJĄCY BĘDZIE KOMUNIKOWAŁ SIĘ Z WYKONAWCAMI, ORAZ INFORMACJE O WYMAGANIACH TECHNICZNYCH I ORGANIZACYJNYCH SPORZĄDZANIA, WYSYŁANIA I ODBIERANIA KORESPONDENCJI ELEKTRONICZNEJ

1. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcami w szczególności składanie oświadczeń, zawiadomień oraz przekazywanie informacji odbywa się elektronicznie za pośrednictwem formularza

„Wyślij wiadomość” dostępnego na stronie profilu nabywcy:

https://platformazakupowa.pl/pn/um_bierutow w zakładce dedykowanej postępowaniu.

2. W postępowaniu o udzielenie zamówienia o wartości mniejszej niż progi unijne ofertę, oświadczenie, o którym mowa w art. 125 ust. 1 ustawy, składa się, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.
3. We wszelkiej korespondencji związanej z niniejszym postępowaniem Zamawiający i Wykonawcy posługują się numerem postępowania określonym przez Zamawiającego na pierwszej stronie SWZ, tj. IR.2710.15.2022.JP.
4. W sytuacjach awaryjnych np. w przypadku przerwy w funkcjonowaniu lub niedziałania https://platformazakupowa.pl/pn/um_bierutow Zamawiający może również komunikować się z Wykonawcami za pomocą poczty elektronicznej, na adres joanna.plociennik@bierutow.pl, z zastrzeżeniem że Ofertę (w szczególności Formularz oferty) wykonawca może złożyć wyłącznie za pośrednictwem Platformy Zakupowej.
5. Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń składane są przez Wykonawcę za pośrednictwem Formularza do komunikacji jako załączniki.
6. Za datę przekazania oświadczeń, wniosków, zawiadomień, dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń oraz innych informacji przyjmuje się datę ich doręczenia za pośrednictwem formularza zamieszczonego na stronie profilu nabywcy https://platformazakupowa.pl/pn/um_bierutow, w zakładce dedykowanej postępowaniu.
7. Wykonawca może zwrócić się do zamawiającego z wnioskiem o wyjaśnienie treści SWZ a Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania odpowiednio ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do zamawiającego nie później niż na 4 dni przed upływem terminu składania odpowiednio ofert.
8. Przedłużenie terminu składania ofert, nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.
9. Treść zapytań wraz z wyjaśnieniami zamawiający przekazuje wykonawcom, którym przekazał specyfikację warunków zamówienia, bez ujawniania źródła zapytania, a jeżeli specyfikacja jest udostępniana na stronie profilu nabywcy, zamieszcza na tej stronie, tj. https://platformazakupowa.pl/pn/um_bierutow, w zakładce dedykowanej postępowaniu.
10. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść specyfikacji warunków zamówienia. Dokonaną zmianę specyfikacji

Zamawiający udostępnia na stronie profilu nabywcy

https://platformazakupowa.pl/pn/um_bierutow, na której udostępniona jest specyfikacja.

11. Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 27 czerwca 2017 r. w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych ze zm. oraz Rozporządzeniu Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy.

Dokumenty w wersji elektronicznej wykonawca sporządza w jednym z formatów zgodnie z Załącznikiem nr 2 do Rozporządzenia 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, tj. Wykazem formatów danych oraz standardów zapewniających dostęp do zasobów informacji udostępnianych za pomocą systemów teleinformatycznych używanych do realizacji zadań publicznych (ze zmianami wprowadzonymi Rozporządzeniem Rady Ministrów z dnia 27 listopada 2014 r. (Dz. U. z 2014 r., poz. 1671) oraz Rozporządzeniem Rady Ministrów z dnia 14 października 2016 r. (Dz. U. z 2016 r., poz. 1 7441).

Zamawiający preferuje sporządzanie dokumentu elektronicznego w postaci .pdf oraz podpisanie kwalifikowanym podpisem elektronicznym w formacie PAdES.

12. Na podstawie ww. rozporządzeń dokumenty lub oświadczenia, o których mowa w rozporządzeniu Ministra Rozwoju, pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia ze zm., składane są w oryginale w postaci dokumentu elektronicznego lub w elektronicznej kopii dokumentu lub oświadczenia poświadczonej za zgodność z oryginałem.
13. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów lub oświadczeń, które każdego z nich dotyczą.
14. Zamawiający może żądać przedstawienia oryginału lub notarialnie poświadczonej kopii dokumentów lub oświadczeń, o których mowa w rozporządzeniu, wyłącznie wtedy, gdy złożona kopia jest nieczytelna lub budzi wątpliwości co do jej prawdziwości.

15. Dokumenty lub oświadczenia, o których mowa w Rozporządzeniu Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy, sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
16. Zgodnie z rozporządzeniem Prezesa RM z 27.06.2017 r. (poz. 1320 ze zm. w 2018r. poz. 1991) w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych:
 - 1) jeżeli oryginał dokumentu lub oświadczenia, o których mowa w art. 125 ust. 1 ustawy, lub inne dokumenty lub oświadczenia składane w postępowaniu o udzielenie zamówienia, nie zostały sporządzone w postaci dokumentu elektronicznego, wykonawca może sporządzić i przekazać elektroniczną kopię posiadanego dokumentu lub oświadczenia,
 - 2) w przypadku przekazywania przez wykonawcę elektronicznej kopii dokumentu lub oświadczenia, opatrzenie jej kwalifikowanym podpisem elektronicznym przez wykonawcę albo odpowiednio przez podmiot, na którego zdolnościach lub sytuacji polega wykonawca na zasadach określonych w art. 22a ustawy, albo przez podwykonawcę jest równoznaczne z poświadczeniem elektronicznej kopii dokumentu lub oświadczenia za zgodność z oryginałem.
17. W przypadku przekazywania przez wykonawcę dokumentu lub dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dane kwalifikowanym podpisem elektronicznym jest równoznaczne z poświadczeniem przez wykonawcę za zgodność z oryginałem wszystkich elektronicznych kopii dokumentów zawartych w tym pliku, z wyjątkiem kopii poświadczonych odpowiednio przez innego wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia, przez podmiot, na którego zdolnościach lub sytuacji polega wykonawca, albo przez podwykonawcę. Do kompresji zamawiający rekomenduje nw. formaty:
 - 1) zip (ZIP file format)
 - 2) .7Z (7-ZIP file format)

ROZDZIAŁ XIX. WSKAZANIE OSÓB UPRAWNIONYCH DO KOMUNIKOWANIA SIĘ Z WYKONAWCAMI

Zamawiający wyznacza następujące osoby do kontaktu z Wykonawcami:

- 1) w sprawach dotyczących przedmiotu zamówienia:
Roman Członkowski – Informatyk – pok. nr 13 budynek A
e-mail: roman.czlonkowski@bierutow.pl

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

Telefon: (71) 3146251, fax: (71) 3146432

2) w sprawach dotyczących organizacji postępowania:

Joanna Płóciennik – Kierownik Referatu IR – pok. nr 01 budynek B

e-mail: joanna.plociennik@bierutow.pl

Telefon: (71) 3146251, fax: (71) 3146432

ROZDZIAŁ XX. OMYŁKI W OFERCIE

1. Zamawiający poprawia w ofercie:
 - 1) oczywiste omyłki pisarskie,
 - 2) oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
 - 3) inne omyłki polegające na niezgodności oferty z dokumentami zamówienia, niepowodujące istotnych zmian w treści oferty
- niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.
2. W przypadku, o którym mowa w ust. 1 pkt 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.

ROZDZIAŁ XXI. WYMAGANIA DOTYCZĄCE WADIUM

Zamawiający odstępuje od żądania wniesienia wadium na podstawie art. 97 ust. 1 ustawy Pzp.

ROZDZIAŁ XXII. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca będzie związany ofertą przez okres **30 dni**, tj. **do dnia 13.08.2022 r.** Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą określonego w SWZ, Zamawiający przed upływem terminu związania ofertą zwraca się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.
3. Przedłużenie terminu związania ofertą, o którym mowa w ust. 2, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

ROZDZIAŁ XXIII. OPIS SPOSOBU PRZYGOTOWANIA OFERT

1. Treść oferty musi odpowiadać treści SWZ. Wykonawcy zobowiązani są zapoznać się dokładnie z treścią niniejszej SWZ i przygotować ofertę zgodnie z wymaganiami w niej określonymi.
2. Oferta musi być sporządzona w języku polskim, w postaci elektronicznej w formacie danych: .pdf, .doc, .docx, .rtf, .xps, .odt i opatrzona kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. W procesie składania oferty na platformie, kwalifikowany podpis elektroniczny Wykonawca składa bezpośrednio na dokumencie, który następnie przesyła do systemu¹ (**opcja rekomendowana** przez platformazakupowa.pl).
3. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą. Poprzez oryginał należy rozumieć dokument podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione. Poświadczenie za zgodność z oryginałem następuje w formie elektronicznej podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione.
4. Oferta powinna być:
 - 1) sporządzona na podstawie załączników niniejszej SWZ w języku polskim,
 - 2) złożona przy użyciu środków komunikacji elektronicznej tzn. za pośrednictwem platformazakupowa.pl,
 - 3) podpisana kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione
5. Do przygotowania oferty konieczne jest posiadanie przez osobę upoważnioną do reprezentowania Wykonawcy kwalifikowanego podpisu elektronicznego, podpisu osobistego lub podpisu zaufanego.
6. Podpisy kwalifikowane wykorzystywane przez wykonawców do podpisywania wszelkich plików muszą spełniać wymogi “Rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku”.

¹ Rozporządzenie Prezesa Rady Ministrów z dnia 27 czerwca 2017 r. w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych.

7. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny. Zamawiający wymaga dołączenia odpowiedniej ilości plików tj. podpisywanych plików z danymi oraz plików podpisu w formacie XAdES.
8. Zgodnie z art. 18 ust. 3 ustawy Pzp, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Jeżeli wykonawca, nie później niż w terminie składania ofert, w sposób niebudzący wątpliwości zastrzegł, że nie mogą być one udostępniane oraz wykazał, załączając stosowne wyjaśnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Na platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.
9. Wykonawca, za pośrednictwem platformazakupowa.pl może przed upływem terminu do składania ofert zmienić lub wycofać ofertę. Sposób dokonywania zmiany lub wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem: <https://platformazakupowa.pl/strona/45-instrukcje>.
10. Każdy z wykonawców może złożyć tylko jedną ofertę dla danej części. Złożenie większej liczby ofert lub oferty zawierającej propozycje wariantowe spowoduje podlegać będzie odrzuceniu.
11. Ceny oferty muszą zawierać wszystkie koszty, jakie musi ponieść wykonawca, aby zrealizować zamówienie z najwyższą starannością oraz ewentualne rabaty.
12. Dokumenty i oświadczenia składane przez wykonawcę powinny być w języku polskim, chyba że w SWZ dopuszczono inaczej. W przypadku załączenia dokumentów sporządzonych w innym języku niż dopuszczony, wykonawca zobowiązany jest załączyć tłumaczenie na język polski.
13. Zgodnie z definicją dokumentu elektronicznego z art. 3 ustęp 2 Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, opatrzenie pliku zawierającego skompresowane dane kwalifikowanym podpisem elektronicznym jest jednoznaczne z podpisaniem oryginału dokumentu, z wyjątkiem kopii poświadczonych odpowiednio przez innego wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia, przez podmiot, na którego zdolnościach lub sytuacji polega wykonawca, albo przez podwykonawcę.
14. Pełnomocnictwo do złożenia oferty musi być złożone w oryginale w takiej samej formie, jak składana oferta (t.j. w formie elektronicznej lub postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym). Dopuszcza się także złożenie elektronicznej kopii (skanu) pełnomocnictwa sporządzonego uprzednio w formie pisemnej, w formie elektronicznego poświadczenia sporządzonego stosownie do art. 97 § 2 ustawy z dnia 14 lutego 1991 r.- Prawo o notariacie, które to poświadczenie notariusz opatruje kwalifikowanym podpisem elektronicznym, bądź też poprzez opatrzenie skanu pełnomocnictwa sporządzonego uprzednio w formie

pisemnej kwalifikowanym podpisem, podpisem zaufanym lub podpisem osobistym mocodawcy. Elektroniczna kopia pełnomocnictwa nie może być uwierzytelniona przez uprawnionego.

15. Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty wynosi 150 MB natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.

ROZDZIAŁ XXIV. SPOSÓB ORAZ TERMIN SKŁADANIA OFERT

1. Ofertę wraz z wymaganymi dokumentami należy umieścić na platformazakupowa.pl pod adresem: https://platformazakupowa.pl/pn/um_bierutow w myśl Ustawy na stronie internetowej prowadzonego postępowania **do dnia 15.07.2022 r. do godz. 08:00**.
2. Do oferty należy dołączyć dokumenty wymagane rozdz. XVI ust. 1 SWZ.
3. Po wypełnieniu Formularza składania oferty lub wniosku i dołączenia wszystkich wymaganych załączników należy kliknąć przycisk „Przejdź do podsumowania”.
4. Oferta składana elektronicznie musi zostać podpisana elektronicznym podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym. W procesie składania oferty za pośrednictwem platformazakupowa.pl, wykonawca powinien złożyć podpis bezpośrednio na dokumentach przesłanych za pośrednictwem platformazakupowa.pl. Zalecamy stosowanie podpisu na każdym załączonym pliku osobno, w szczególności wskazanych w art. 63 ust 1 oraz ust.2 Pzp, gdzie zaznaczono, iż oferty, wnioski o dopuszczenie do udziału w postępowaniu oraz oświadczenie, o którym mowa w art. 125 ust.1 sporządza się, pod rygorem nieważności, w postaci lub formie elektronicznej i opatruje się odpowiednio w odniesieniu do wartości postępowania kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
5. Za datę złożenia oferty przyjmuje się datę jej przekazania w systemie (platformie) w drugim kroku składania oferty poprzez kliknięcie przycisku “Złóż ofertę” i wyświetlenie się komunikatu, że oferta została zaszyfrowana i złożona.
6. Szczegółowa instrukcja dla Wykonawców dotycząca złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem: <https://platformazakupowa.pl/strona/45-instrukcje>
7. W związku z tym, że Zamawiający nie odpowiada za ewentualną awarię internetu, czy problemy techniczne powstałe u Wykonawcy, zaleca zaplanowanie złożenia Oferty z odpowiednim wyprzedzeniem.
8. W przypadku pytań dotyczących funkcjonowania i obsługi technicznej platformy, prosimy o skorzystanie z pomocy **Centrum Wsparcia Klienta**, które udziela wszelkich informacji związanych z procesem składania ofert, rejestracji czy innych aspektów technicznych platformy, dostępne codziennie od poniedziałku do piątku w godz. od 7.00 do 17.00 pod nr tel. 22 101-02-02.

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

ROZDZIAŁ XXV. TERMIN OTWARCIA OFERT

1. Otwarcie ofert nastąpi w dniu **15.07.2022 r., o godzinie 08:05.**
2. Otwarcie ofert jest niejawne.
3. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
4. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o:
 - 1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
 - 2) cenach lub kosztach zawartych w ofertach.Informacja zostanie opublikowana na stronie postępowania na platformazakupowa.pl w sekcji „Komunikaty” .
5. W przypadku wystąpienia awarii systemu teleinformatycznego, która spowoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
6. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
7. W przypadku ofert, które podlegają negocjacjom, zamawiający udostępnia informacje, o których mowa w ust. 4 pkt 2, niezwłocznie po otwarciu ofert ostatecznych albo unieważnieniu postępowania.

ROZDZIAŁ XXVI. SPOSÓB OBLICZENIA CENY

1. Wykonawca podaje cenę oferty w Formularzu Ofertowym sporządzonym według wzoru stanowiącego Załącznik Nr 1 do SWZ, jako cenę brutto [z uwzględnieniem kwoty podatku od towarów i usług (VAT)] z wyszczególnieniem stawki podatku od towarów i usług (VAT).
2. Cena oferty stanowi wynagrodzenie ryczałtowe.
3. Cena musi być wyrażona w złotych polskich (PLN), z dokładnością nie większą niż dwa miejsca po przecinku.
4. Wykonawca podaje w Formularzu Ofertowym stawkę podatku od towarów i usług (VAT) właściwą dla przedmiotu zamówienia, obowiązującą według stanu prawnego na dzień składania ofert. Określenie ceny ofertowej z zastosowaniem nieprawidłowej stawki podatku od towarów i usług (VAT) potraktowane będzie, jako błąd w obliczeniu ceny i spowoduje odrzucenie oferty, jeżeli nie ziszczą się ustawowe przesłanki omyłki (na podstawie art. 226 ust. 1 pkt 10 pzp w związku z art. 223 ust. 2 pkt 3 pzp).
5. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

polskich (PLN).

6. W przypadku rozbieżności pomiędzy ceną ryczałtową podaną cyfrowo a słownie, jako wartość właściwa zostanie przyjęta cena ryczałtowa podana słownie.

ROZDZIAŁ XXVII. OPIS KRYTERIÓW OCENY OFERT, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW, I SPOSOBU OCENY OFERT

1. Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami: cena oraz termin wykonania dostawy.
2. Oferty zostaną ocenione za pomocą systemu punktowego, zgodnie z poniższymi kryteriami:

Kryterium: Cena – 60%

Maksymalną liczbę punktów (60) otrzyma Wykonawca, który zaproponuje najniższą całkowitą cenę za realizację zamówienia, natomiast pozostali Wykonawcy otrzymają odpowiednio mniejszą liczbę punktów zgodnie z poniższym wzorem:

P – liczba punktów przyznanych Wykonawcy za Cenę

$$P = C_N / C_{OB} \times 60$$

gdzie:

C_N – najniższa zaoferowana Cena,

C_{OB} – Cena zaoferowana w ofercie badanej.

Kryterium: Termin wykonania przedmiotu umowy – 40%

T – liczba punktów przyznanych Wykonawcy za termin wykonania

- 1) Wykonawca, który zaproponuje skrócenie terminu o 30 dni otrzyma 40 pkt
- 2) Wykonawca, który zaproponuje skrócenie terminu o 15 dni otrzyma 20 pkt
- 3) Wykonawca, który zaproponuje termin wynikający z SWZ otrzyma 0 pkt

Sumaryczna liczba punktów zostanie obliczona wg następującego wzoru:

$$\text{Ilość punktów} = P + T$$

3. Ocenie będą podlegać wyłącznie oferty nie podlegające odrzuceniu.
4. Za najkorzystniejszą zostanie uznana oferta, która uzyskana największą sumaryczną ilość punktów.
5. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

dotyczących treści złożonych przez nich ofert lub innych składanych dokumentów lub oświadczeń. Wykonawcy są zobowiązani do przedstawienia wyjaśnień w terminie wskazanym przez Zamawiającego.

ROZDZIAŁ XXVIII. WYBÓR NAJKORZYSTNIEJSZEJ OFERTY

1. Wykonawca jest związany ofertą do upływu terminu określonego datą w dokumentach zamówienia, jednak nie dłużej niż 30 dni od dnia upływu terminu składania ofert, przy czym pierwszym dniem terminu związania ofertą jest dzień, w którym upływa termin składania ofert.
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą określonego w dokumentach zamówienia, zamawiający przed upływem terminu związania ofertą zwraca się jednokrotnie do wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.
3. Przedłużenie terminu związania ofertą, o którym mowa w ust. 2, wymaga złożenia przez wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.
4. W przypadku gdy zamawiający żąda wniesienia wadium, przedłużenie terminu związania ofertą, o którym mowa w ust. 2, następuje wraz z przedłużeniem okresu ważności wadium albo, jeżeli nie jest to możliwe, z wniesieniem nowego wadium na przedłużony okres związania ofertą.

ROZDZIAŁ XXIX. INFORMACJE O FORMALNOŚCIACH, JAKIE MUSZĄ ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Zamawiający zawiera umowę w sprawie zamówienia publicznego, z uwzględnieniem art. 577 pzp, **w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty**, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 10 dni, jeżeli zostało przesłane w inny sposób.
2. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 1, jeżeli w postępowaniu o udzielenie zamówienia złożono tylko jedną ofertę.
3. Wykonawca, którego oferta została wybrana jako najkorzystniejsza, zostanie poinformowany przez Zamawiającego o miejscu i terminie podpisania umowy.
4. Wykonawca, o którym mowa w ust. 1, ma obowiązek zawrzeć umowę w sprawie zamówienia na warunkach określonych w projektowanych postanowieniach umowy, które stanowią załącznik nr 5 do SWZ. Umowa zostanie uzupełniona o zapisy

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

wynikające ze złożonej oferty.

5. Przed podpisaniem umowy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (w przypadku wyboru ich oferty jako najkorzystniejszej) przedstawią Zamawiającemu umowę regulującą współpracę tych Wykonawców.
6. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców albo unieważnić postępowanie.

ROZDZIAŁ XXX. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający nie przewiduje wniesienia zabezpieczenia w niniejszym postępowaniu.

ROZDZIAŁ XXXI. INFORMACJE O TREŚCI ZAWIERANEJ UMOWY ORAZ MOŻLIWOŚCI JEJ ZMIANY

1. Wybrany Wykonawca jest zobowiązany do zawarcia umowy w sprawie zamówienia publicznego na warunkach określonych we wzorze umowy, stanowiącym załącznik nr 5 do SWZ.
2. Zakres świadczenia Wykonawcy wynikający z umowy jest tożsamy z jego zobowiązaniem zawartym w ofercie.
3. Zamawiający przewiduje możliwość zmiany zawartej umowy w stosunku do treści wybranej oferty w zakresie uregulowanym w art. 454-455 pzp oraz wskazanym we wzorze umowy, stanowiącym załącznik nr 5 do SWZ.
4. Zmiana umowy wymaga dla swej ważności, pod rygorem nieważności, zachowania formy pisemnej.

ROZDZIAŁ XXXII. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

1. Środki ochrony prawnej przysługują Wykonawcy, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów pzp.
2. Odwołanie przysługuje na:
 - 1) niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia,
 - 2) zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której Zamawiający był obowiązany na podstawie ustawy.
3. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej.

4. Na orzeczenie Krajowej Izby Odwoławczej oraz postanowienie Prezesa Krajowej Izby Odwoławczej, o którym mowa w art. 519 ust. 1 pzp, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargę wnosi się do Sądu Okręgowego w Warszawie za pośrednictwem Prezesa Krajowej Izby Odwoławczej.
5. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX „Środki ochrony prawnej” pzp.

ROZDZIAŁ XXXIII. ZAŁĄCZNIKI DO SWZ

Integralną częścią niniejszej SWZ stanowią następujące załączniki:

- 1) Formularz ofertowy – załącznik nr 1;
- 2) Oświadczenie o braku podstaw do wykluczenia i o spełnianiu warunków udziału w postępowaniu – załącznik nr 2;
- 3) Oświadczenie podmiotu udostępniającego zasoby uwzględniające przesłanki wykluczenia z art. 7 ust. 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego składane na podstawie art. 125 ust. 5 ustawy Pzp – załącznik nr 3;
- 4) Opis przedmiotu zamówienia (parametry techniczno-użytkowe) – załącznik nr 4a-4g;
Załącznik Nr 4a – Opis przedmiotu zamówienia – część nr 1;
Załącznik Nr 4b – Opis przedmiotu zamówienia – część nr 2;
Załącznik Nr 4c – Opis przedmiotu zamówienia – część nr 3;
Załącznik Nr 4d – Opis przedmiotu zamówienia – część nr 4;
Załącznik Nr 4e – Opis przedmiotu zamówienia – część nr 5;
Załącznik Nr 4f – Opis przedmiotu zamówienia – część nr 6;
Załącznik Nr 4g – Opis przedmiotu zamówienia – część nr 7;
- 5) Wzór ogólnych warunków umowy – załącznik nr 5;
- 6) Wzór umowy o powierzenie przetwarzania danych osobowych – załącznik nr 6;
- 7) Zobowiązanie innego podmiotu do udostępnienia niezbędnych zasobów Wykonawcy – załącznik nr 7;
- 8) Oświadczenie dotyczące przynależności lub braku przynależności do tej samej grupy kapitałowej – załącznik nr 8;
- 9) Klauzula informacyjna – załącznik nr 9.

Załącznik Nr 1 – do SWZ
Formularz ofertowy

województwo	
powiat	
REGON	
NIP	
osoba do kontaktu	
tel., fax	
Tel. Kom.	
e-mail	

MIASTO I GMINA BIERUTÓW
ul. Moniuszki 12
56-420 Bierutów

OFERTA

Ja (my) niżej podpisany(i)	
działając w imieniu i na rzecz	

nawiązując do toczącego się postępowania o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym z możliwością negocjacji pn.: **Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” – nr sprawy: IR.2710.15.2022.JP**

1. Oświadczamy, że wykonamy dostawę za następującą sumaryczną wartość ryczałtową:

wartość brutto	
słownie złotych brutto	
wartość netto	
podatek VAT %	

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

w tym:

Część nr 1 – Zakup serwerów*:

L.p.	Przedmiot dostawy	Cena jednostkowa netto (zł)	Liczba sztuk ogółem	Cena łączna netto (kol.3 x kol.4)	Kwota VAT	Kwota ogółem brutto (zł) (kol.5 + kol.6)
1	2	3	4	5	6	7
1.	Serwer producent:* model:* (* wypełnia Wykonawca)		2			
Cena ogółem brutto (część nr 1) wynosi:						

Część nr 2 – Modernizacja wewnętrznej sieci LAN*:

L.p.	Przedmiot dostawy	Cena jednostkowa netto (zł)	Liczba sztuk ogółem	Cena łączna netto (kol.3 x kol.4)	Kwota VAT	Kwota ogółem brutto (zł) (kol.5 + kol.6)
1	2	3	4	5	6	7
1.	Modernizacja wewnętrznej sieci LAN:* (* wypełnia Wykonawca)		1			
Cena ogółem brutto (część nr 2) wynosi:						

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Część nr 3 – Zakup urządzenia wielofunkcyjnego z możliwością skanowania do sieci*:

L.p.	Przedmiot dostawy	Cena jednostkowa netto (zł)	Liczba sztuk ogółem	Cena łączna netto (kol.3 x kol.4)	Kwota VAT	Kwota ogółem brutto (zł) (kol.5 + kol.6)
1	2	3	4	5	6	7
1.	<p>Sieciowe urządzenie wielofunkcyjne producent:</p> <p>model:</p> <p>(* wypełnia Wykonawca)</p>		1			
Cena ogółem brutto (część nr 3) wynosi:						

Część nr 4 – Zakup oprogramowania biurowego*:

L.p.	Przedmiot dostawy	Cena jednostkowa netto (zł)	Liczba licencji ogółem	Cena łączna netto (kol.3 x kol.4)	Kwota VAT	Kwota ogółem brutto (zł) (kol.5 + kol.6)
1	2	3	4	5	6	7
1.	Oprogramowanie Microsoft 365 Standard		40			
2.	Oprogramowanie Microsoft 365 Basic		50			
Cena ogółem brutto (część nr 4) wynosi: (suma wierszy 1 – 2 z kolumny nr 7)						

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Część nr 5 – Zakup systemu do tworzenia kopii bezpieczeństwa*:

L.p.	Przedmiot dostawy	Cena jednostkowa netto (zł)	Liczba sztuk ogółem	Cena łączna netto (kol.3 x kol.4)	Kwota VAT	Kwota ogółem brutto (zł) (kol.5 + kol.6)
1	2	3	4	5	6	7
1.	Oprogramowanie do backup producent:* nazwa:* (* wypełnia Wykonawca)		1			
2.	Urządzenie do przechowywania kopii danych producent:* nazwa:* (* wypełnia Wykonawca)		1			
Cena ogółem brutto (część nr 5) wynosi: (suma wierszy 1 – 2 z kolumny nr 7)						

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Część nr 6 – Zakup oprogramowania do monitorowania urządzeń sieciowych*:

L.p.	Przedmiot dostawy	Cena jednostkowa netto (zł)	Liczba licencji ogółem	Cena łączna netto (kol.3 x kol.4)	Kwota VAT	Kwota ogółem brutto (zł) (kol.5 + kol.6)
1	2	3	4	5	6	7
1.	Oprogramowanie do ochrony danych i inwentaryzacji sieciowej producent:* nazwa:* (* wypełnia Wykonawca)		50			
Cena ogółem brutto (część nr 6) wynosi:						

Część nr 7 – Zakup oprogramowania i urządzenia do ochrony brzegu sieci*:

L.p.	Przedmiot dostawy	Cena jednostkowa netto (zł)	Liczba sztuk ogółem	Cena łączna netto (kol.3 x kol.4)	Kwota VAT	Kwota ogółem brutto (zł) (kol.5 + kol.6)
1	2	3	4	5	6	7
1.	Oprogramowanie i urządzenie do ochrony brzegu sieci producent:* nazwa:* (* wypełnia Wykonawca)		1			
Cena ogółem brutto (część nr 7) wynosi:						

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

2. Wymagania Zamawiającego dotyczące zakresu przedmiotu zamówienia:

- Tabela nr 1: Zestawienie parametrów technicznych oferowanych serwerów*.
 Tabela nr 2: Zestawienie parametrów modernizacji wewnętrznej sieci LAN*.
 Tabela nr 3: Zestawienie parametrów technicznych oferowanego Sieciowego urządzenia wielofunkcyjnego*.
 Tabela nr 4: Zestawienie parametrów technicznych oferowanego Oprogramowania biurowego*.
 Tabela nr 5: Zestawienie parametrów technicznych oferowanego systemu do tworzenia kopii bezpieczeństwa*.
 Tabela nr 6: Zestawienie parametrów technicznych oferowanego oprogramowania do monitorowania urządzeń sieciowych*.
 Tabela nr 7: Zestawienie parametrów technicznych oferowanego oprogramowania i urządzenia do ochrony brzegu sieci*.

Tabela nr 1: Zestawienie parametrów technicznych oferowanych serwerów*

L.p.	Nazwa parametru	Wartości minimalne wymagane przez Zamawiającego	Wartości oferowane przez Wykonawcę (tę kolumnę wypełnia Wykonawca) ²
1	2	3	4 Proszę podać nazwę producenta i typ/model oferowanego urządzenia:
1	Procesor	Zainstalowany jeden procesor sześciordzeniowy dedykowany do pracy z zaoferowanym serwerem, taktowany zegarem min 2.9 GHz (częstotliwość bazowa) umożliwiające osiągnięcie wyniku minimum 16 600 punktów w teście	(UWAGA: Należy również podać nazwę producenta oraz model oferowanego procesora) Producent: Model:

2 Jeśli Wykonawca oferuje sprzęt w pełni odpowiadający wymaganiom opisanym w kol. „Wartości minimalne wymagane przez Zamawiającego”, wówczas w kol. „Wartości oferowane przez Wykonawcę” należy wpisać: „TAK”. Jeśli natomiast Wykonawca oferuje sprzęt o innych parametrach niż opisane w kol. „Wartości minimalne wymagane przez Zamawiającego”, wówczas w kol. „Wartości oferowane przez Wykonawcę” należy opisać wartości oferowane przez Wykonawcę.

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		PassMark - CPU Mark dostępnym na stronie internetowej https://www.cpubenchmark.net/high_end_cpus.html z dnia 01.06.2022 r.
2	Płyta główna	Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.	Producent:
3	Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych	
4	Obudowa	Obudowa Rack 19" o wysokości max 1U z możliwością instalacji 8 dysków 2,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.	
5	RAM	64 GB pamięci RAM ECC UDIMM w kościach 32GB o częstotliwości pracy 3200MT/s. Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci	Zainstalowana pamięć RAM: Obsługiwana pamięć RAM:
6	Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200	
7	Gniazda PCI	Min. 2 sloty PCIe generacji 4	
8	Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

9	Wbudowane porty	min. 4 porty USB w tym min. 1 port USB 3.0 z tyłu obudowy, 1 port VGA na tylnym panelu, min. 1 port RS232	
10	Kontroler dysków	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfujących.	
11	Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD, NL SAS Zainstalowane 2 dyski SSD SATA o pojemności min. 960GB, 6Gb, Hot-Plug o parametrze DWPD wynoszącym min. 1. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.	
12	System diagnostyczny	Diody LED informujące o kondycji serwera.	
13	Wentylatory	Minimum 4 wentylatory	
14	Zasilacze	Dwa zasilacze o mocy min. 600W	

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

15	System operacyjny/ dodatkowe oprogramowanie	Zainstalowany fabrycznie Windows Serwer w wersji 2022 Standard	
16	Bezpieczeństwo	Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardej. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem	
17	Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.	
18	Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<ol style="list-style-type: none"> 1) zdalny dostęp do graficznego interfejsu Web karty zarządzającej; 2) zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); 3) szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; 4) wsparcie dla IPv6; 5) wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; 6) możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; 7) integracja z Active Directory; 8) wsparcie dla dynamic DNS; 9) wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. 10) możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera 11) możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera 	
19	Gwarancja	min. 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia,	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

20	Certyfikaty	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001.</p> <p>Serwer musi posiadać deklaracja CE.</p> <p>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022</p>	
21	Dokumentacja	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela</p>	
22	Dodatkowe informacje	<p>Urządzenie musi być fabrycznie nowe, wcześniej nie używane, z wszystkimi standardowo dołączanymi przez producenta elementami oraz pochodzić z oficjalnego kanału sprzedaży.</p>	

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Tabela nr 2: Zestawienia parametrów modernizacji wewnętrznej sieci LAN*

L.p.	Nazwa parametru	Wartości minimalne wymagane przez Zamawiającego	Wartości oferowane przez Wykonawcę (tę kolumnę wypełnia Wykonawca) ³
1	Ilość punktów elektryczno-logicznych (PEL)	50 PEL (Szczegółowa lokalizacja PEL zostanie wskazana na etapie opracowania projektu wykonawczego)	
2	Elementy składowe każdego punktu elektryczno-logicznego (PEL)	1) dwa gniazda RJ45 (montowane w kanałach instalacyjnych natynkowych) kategorii 6a lub wyższej oraz 2) dwa gniazda elektryczne 230V (montowane w korycie) z blokadą uniemożliwiającą podłączenie nieuprawnionych odbiorników	
3	Wymagania dotyczące dostarczonej szafy serwerowej	1) Wysokość 37U (max 1800 mm), 2) Szerokość nie mniej niż 600x800 mm, 3) Wyposażenie szafy: a) panel wentylacyjny, b) panele krosowe modułowe kat.6, c) panele z przewodnikami kabla w ilości równej panelom krosowniczym, d) 2 listwy zasilające, e) 2 półki o głębokości min 600 mm i obciążalności	

³ Jeśli Wykonawca oferuje sprzęt w pełni odpowiadający wymaganiom opisanym w kol. „Wartości minimalne wymagane przez Zamawiającego”, wówczas w kol. „Wartości oferowane przez Wykonawcę” należy wpisać: „TAK”. Jeśli natomiast Wykonawca oferuje sprzęt o innych parametrach niż opisane w kol. „Wartości minimalne wymagane przez Zamawiającego”, wówczas w kol. „Wartości oferowane przez Wykonawcę” należy opisać wartości oferowane przez Wykonawcę.

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>min 80 kg,</p> <p>4) Konfiguracja szafy:</p> <p>a) standardowo wyposażona przez producenta w drzwi przednie oszklone z możliwością zmiany strony mocowania,</p> <p>b) zdejmowane osłony boczne,</p> <p>c) możliwość wyprowadzenia kabli przez podłogę sufit oraz tył szafy,</p> <p>d) profile montażowe regulowane,</p> <p>e) inne, standardowe dołączane przez producenta wyposażenie</p>	
4	<p>Prace przewidziane w ramach instalacji okablowania strukturalnego</p>	<p>1) budowa nowych tras kablowych,</p> <p>2) układanie kabli w nowych i istniejących trasach,</p> <p>3) instalacja punktów PEL - (punkt elektryczno-logiczny),</p> <p>4) montaż paneli krosowych 48xRJ45 w szafie serwerowej i ewentualnych szafach dystrybucyjnych,</p> <p>5) dostarczenie i montaż szafy serwerowej i ewentualnych szaf dystrybucyjnych oraz patchpaneli krosowych RJ45 kat. 6; ilość paneli należy dostosować do liczby instalowanych gniazd z zapewnieniem 50% nadmiarowości,</p> <p>6) terminowanie kabli w</p>	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		osprzęcie przyłączeniowym, 7) pomiary tras kablowych, wykonanie dokumentacji powykonawczej	
5	Wymagane parametry funkcjonalno-użytkowe okablowania strukturalnego	1)system okablowania strukturalnego co najmniej kategorii 6a musi zapewnić możliwość transmisji głosu, danych, sygnałów wideo, 2)w okablowaniu muszą być zastosowane 4-parowe kable symetryczne UTP, które charakteryzują się parametrami i jakością niezbędną do prawidłowej pracy systemu zarówno w chwili obecnej, jak i w przyszłości, 3)budowane trasy mają być prowadzone w kanale instalacyjnym natynkowym (korytka PCV), 4)izolacja zewnętrzna okablowania miedzianego musi być wykonana z PVC lub z materiału LSZH nie wydzielającego toksycznych oparów podczas spalania (nie zawiera halogenu), 5)w okablowaniu wszystkie komponenty (w tym parametry transmisyjne) muszą charakteryzować się pełną zgodnością ze specyfikacją dla kategorii 6, 6)moduły RJ45 powinny być zarabiane narzędziowo,	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>7) gniazda naścienne i na panelu krosowym muszą być oznaczone tj. posiadać czytelną numerację na obydwu końcach toru,</p> <p>8) wymiar panelu krosowego musi być następujący - szerokość 19", max wysokość 2 U,</p> <p>9) panel musi umożliwić zamontowanie min. 24 modułów RJ45,</p> <p>10) okablowanie musi bazować na jednorodnym rozwiązaniu systemu okablowania strukturalnego, którego wszystkie elementy toru transmisyjnego pochodzą od tego samego producenta.</p>	
6	<p>Wymagania dotyczące wykonania dedykowanej instalacji elektrycznej</p>	<p>1) rozbudowa instalacji elektrycznej gniazd wtykowych zasilania dedykowanego – dwa gniazda na PEL,</p> <p>2) rozbudowa istniejących rozdzielnic lub ich wymiany (w przypadku braku możliwości rozbudowy),</p> <p>3) wykonania dedykowanej instalacji zasilającej w układzie TN-S,</p> <p>4) wszystkie gniazda elektrycznej sieci zasilającej, powinny posiadać zabezpieczenie w postaci klucza typu DATA, aby</p>	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>uniemożliwić podłączenia dowolnych urządzeń elektrycznych i tym samym wprowadzić podniesienie bezpieczeństwa użytkowania. Wymagane jest dostarczenie kluczy w ilości odpowiadającej zainstalowanym gniazdom,</p> <p>5) do budowy toru zasilającego koniecznym jest użycie przewodów izolowanych YDY – 750V, 3x2,5 mm² lub innych o porównywalnych parametrach izolacyjno-eksploatacyjnych,</p> <p>6) obwody elektryczne w obrębie pomieszczeń mają być prowadzone łącznie z instalacją logiczną w kanale instalacyjnym natynkowym (korytka PCV) - rozdzielone przegrodą lub w odrębnych kanałach,</p> <p>7) należy zaprojektować max. 5 urządzeń na jeden obwód zabezpieczający,</p> <p>8) każdy obwód elektryczny musi zostać zabezpieczony wyłącznikiem przepięciowym i różnicowo-prądowym. Instalację należy zasilić z dedykowanej rozdzielni głównej budynku.</p> <p>Od istniejących tablic rozdzielczych zostanie</p>	
--	--	--	--

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

	<p>wykonane zasilanie YDY-žo 5x10mm.</p> <p>Do instalacji zostanie zamontowany podlicznik energii elektrycznej.</p> <p>Dla poprawienia wartości uziomu, który nie powinien przekraczać wartości 10Ω, jeżeli zajdzie taka potrzeba, zostanie wbity pręty pomiedziowane typu galmar, w okolicy istniejącego złącza kablowego na zewnątrz budynku, aby zapewnić prawidłowe funkcjonowanie ochrony TN-S w całym obiekcie.</p> <p>W istniejących tablicach elektrycznych zostaną umieszczone zabezpieczenia gniazd zasilania komputerowego.</p> <p>Szafa serwerowa będzie podłączona do osobnego zabezpieczenia przepięciowego i różnicowo-prądowego.</p> <p>W przypadku, gdy istniejące tablice okażą się za małe, zostaną wymienione na nowe.</p> <p>Instalacja gniazd wtyczkowych zostanie wykonana przewodami</p>	
--	--	--

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>miedzianymi typu YDY-žo 3x750V o przekroju 2,5 mm. z osobną żyłą „N” i PE. Wszystkie gniazda wtyczkowe będą posiadać bolec ochronny.</p> <p>Obwód gniazd komputerowych 230V, w tablicach elektrycznych zostanie zabezpieczony wyłącznikiem różnicowo-prądowym 16A, $\Delta I=0,03A$, o charakterystyce typu „A”.</p> <p>Jako dodatkową ochronę od porażień prądem elektrycznym po stronie nn-0,4kV zastosowane zostaną „samoczynne wyłączanie zasilania” w układzie TN-C-S (dla sieci zasilającej układ TN-C, dla odbiorczej TN-S). W celu zapewnienia ochrony przepięciowej, zastosowane zostaną odgromniki 4xDEHNbloc i ochronniki przepięciowe 4xDEHNquard. Dla prawidłowego funkcjonowania ochrony przepięciowej zastosowany zostanie dławiki typu DEHNbridge</p>	
7	Gwarancja	min. 5 lat na wykonaną instalację oraz dostarczony sprzęt	
8	Dodatkowe informacje	Elementy PEL (puntów elektryczno-logicznych) oraz szafy serwerowej muszą być	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		fabrycznie nowe, wcześniej nie używane, dostarczone z wszystkimi standardowo dołączanymi przez producenta elementami.	
--	--	---	--

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Tabela nr 3: Zestawienie parametrów technicznych oferowanego Sietowego urządzenia wielofunkcyjnego*

Nazwa parametru lub wymaganej funkcji		Wartości minimalne wymagane przez Zamawiającego	Wartości oferowane przez Wykonawcę (tę kolumnę wypełnia Wykonawca) ⁴ Proszę podać producenta i model oferowanego urządzeniach
Technologia druku		technologia laserowa	
Format skanowanego oryginału		A3	
Format kopii		A3-A6	
Prędkość drukowania	A4	nie mniej niż 26 stron/min.	
	A3	nie mniej niż 15 stron/min.	
Obsługiwane rozdzielczości drukowania		Nie gorsza niż 1200x600 dpi oraz 600x600 dpi	
Czas wydruku pierwszej strony		maks. 5 sek.	
Czas nagrzewania		maks. 20 sek. od włączenia zasilania	
Kopiowanie wielokrotne		do 999 kopii	
Pamięć RAM		min. 2 GB	
Dysk HDD lub SSD		min. 30 GB	
Zoom		25-400%	
Panel operatora		Panel wyposażony w kolorowy ekran dotykowy LCD, min. 7-calowy, opisy	

4 Jeśli Wykonawca oferuje sprzęt w pełni odpowiadający wymaganiom opisanym w kol. „Wartości minimalne wymagane przez Zamawiającego”, wówczas w kol. „Wartości oferowane przez Wykonawcę” należy wpisać: „TAK”. Jeśli natomiast Wykonawca oferuje sprzęt o innych parametrach niż opisane w kol. „Wartości minimalne wymagane przez Zamawiającego”, wówczas w kol. „Wartości oferowane przez Wykonawcę” należy opisać wartości oferowane przez Wykonawcę.

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

	na panelu oraz komunikaty na ekranie w języku polskim.	
Dupleks	Automatyczny, obsługa papieru 60-160 g/m ²	
Podajnik dokumentów	Automatyczny dwustronny, taca podającej na min. 140 ark. 80 g/m ²	
Podajnik papieru	podajnik o pojemności min. 2 x 500 ark. A5-A3 (80 g/m ²), 60-160 g/m ² taca boczna, min. 100 ark. A6-A3 (80 g/m ²), 60-250 g/m ²	
Odbiornik wydruków i kopii	Taca odbiorcza na min. 250 ark. (80 g/m ²)	
Podstawa na kółkach	Dedykowana podstawa producenta urządzenia z katalogu dostępnych fabrycznie opcji, zamykana, na kółkach. Dopasowana kolorystycznie, wzorniczo i kształtem do obudowy urządzenia.	
Pamięć drukarki	Współdzielona z kopiarką (dotyczy pamięci RAM i dysku)	
Emulacje	PCL 6, PostScript Level 3	
Interfejsy	USB 2.0 Ethernet 10/100/1000Base-T	
Funkcje skanowania	skanowanie do PC, do e-mail, do FTP, sieciowy TWAIN, do pamięci przenośnej USB, WIA, SMB, do skrzynki dokumentów	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Rozdzielczość skanowania	600 dpi lub lepsza	
Prędkość skanowania	min. 80 str. / min. (A4, kolor, 300 dpi)	
Typy plików	PDF, JPEG, TIFF, XPS, PDF szyfrowany, PDF/A	
Materiały eksploatacyjne jako wyposażenie standardowe (dostarczone w komplecie w ramach oferowanej ceny jednostkowej).	Tonery: w ilości, która zapewni wydrukowanie minimum 20 000 stron A4 (zgodnie z ISO 19752) Bębny: w ilości, która zapewni wydrukowanie minimum 600 000 stron A4. Dostarczone materiały muszą być nowe, nieregenerowane i wyprodukowane przez producenta oferowanych urządzeń.	
Możliwość rozbudowy	- Podajnik papieru na min. 3000 ark. A4, 80 g/m ² ; - finiszier zszywający, min. 2 tace odbiorcze o łącznej pojemności min. 3.000 ark. A4-80 g/m ² , obsługa papieru o wadze 60-250 g/m ² , - zszywacz min. 50 ark., dziurkacz 2/4;	
Funkcja dodatkowa	Urządzenie wyposażone w funkcję zgłaszania usterek bezpośrednio z panelu dotykowego urządzenia.	
Wymagania dodatkowe	Oferent musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzenia	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

	wielofunkcyjnego - dokumenty potwierdzające dołączyć do oferty	
	Certyfikat ISO 9001:2015 producenta oferowanego sprzętu - dokument potwierdzający załączyć do oferty	
	Certyfikat ISO 14001:2015 producenta oferowanego sprzętu - dokument potwierdzający załączyć do oferty	
	Oświadczenie producenta oferowanego sprzętu lub jego autoryzowanego przedstawiciela w Polsce, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Konieczność nie zachodzi w przypadku autoryzowanego przedstawiciela producenta.	
	Urządzenie musi być fabrycznie nowe, wcześniej nie używane, dostarczone z wszystkimi standardowo oferowanymi przez producenta elementami i pochodzić z oficjalnego kanału sprzedaży.	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Gwarancja	Gwarancja producenta nie mniej 24 miesięcy	
------------------	--	--

Tabela nr 4: Zestawienie parametrów technicznych oferowanego Oprogramowania biurowego*

L.p.	Nazwa parametru	Wartości minimalne wymagane przez Zamawiającego	Wartości oferowane przez Wykonawcę (tę kolumnę wypełnia Wykonawca) ⁵
1	2	3	4
1	Oprogramowanie biurowe (50 stanowisk)	Oprogramowanie biurowe Microsoft 365 Business Basic.	
2	Oprogramowanie biurowe (40 stanowisk)	Oprogramowanie biurowe Microsoft 365 Business Standard.	
3	Zastosowanie	Dla jednostek administracji samorządowej	
4	Okres licencji	18 miesięcy	
5	Wersja językowa	Polska	

⁵ Jeśli Wykonawca oferuje sprzęt w pełni odpowiadający wymaganiom opisanym w kol. „Wartości minimalne wymagane przez Zamawiającego”, wówczas w kol. „Wartości oferowane przez Wykonawcę” należy wpisać: „TAK”. Jeśli natomiast Wykonawca oferuje sprzęt o innych parametrach niż opisane w kol. „Wartości minimalne wymagane przez Zamawiającego”, wówczas w kol. „Wartości oferowane przez Wykonawcę” należy opisać wartości oferowane przez Wykonawcę.

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Tabela nr 5: Zestawienie parametrów technicznych oferowanego systemu do tworzenia kopii bezpieczeństwa*

Nazwa parametru	Wartości minimalne wymagane przez Zamawiającego	Wartości oferowane przez Wykonawcę (tę kolumnę wypełnia Wykonawca) ⁶
1	2	3
Opis ogólny	<p>Kompleksowe, zintegrowane rozwiązanie do backupu wraz z usługą wdrożenia zdalnego oraz pomocą techniczną wykonawcy na okres 1 roku.</p> <p>W zastosowanym rozwiązaniu oprogramowanie do centralnego zarządzania backupem ma być zintegrowane z platformą sprzętową serwera NAS tak aby nie było potrzeby instalacji serwera backupu (serwera zarządzania) na osobnym serwerze klienta.</p> <p>System powinien umożliwić archiwizację 40 stacji roboczych 2 serwery (Windows Server) oraz 4 hosty Hyper-V.</p> <p>Zamawiający wymaga dostarczenia i wdrożenia rozwiązania składającego się z urządzenia NAS, dysków twardych oraz oprogramowania do backupu spełniających poniższe wymagania.</p>	
Minimalna specyfikacja platformy sprzętowej:		
Procesor	Jeden 4-rdzeniowy/4-wątkowy Intel Celeron N5105/N5095 lub równoważny procesor osiągający	

⁶ Jeśli Wykonawca oferuje sprzęt w pełni odpowiadający wymaganiom opisanym w kol. „Wartości minimalne wymagane przez Zamawiającego”, wówczas w kol. „Wartości oferowane przez Wykonawcę” należy wpisać: „TAK”. Jeśli natomiast Wykonawca oferuje sprzęt o innych parametrach niż opisane w kol. „Wartości minimalne wymagane przez Zamawiającego”, wówczas w kol. „Wartości oferowane przez Wykonawcę” należy opisać wartości oferowane przez Wykonawcę.

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

	<p>w testach PassMark - CPU Mark wynik nie gorszy niż 4000 pkt.</p> <p>W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie https://www.cpubenchmark.net</p>	
Obudowa	Rack 2U o wymiarach nie większych niż, 87× 483 × 347 mm (wys. x szer. x gł.); w zestawie szyny wysuwane do instalacji w szafie RACK	
Pamięć RAM	4 GB SODIMM DDR4 Urządzenie powinno obsługiwać do 16GB pamięci RAM.	
Ilość obsługiwanych dysków	8 dysków 3,5-calowych 3,5/2,5 dyski SATA	
Zamontowane dyski twarde	Zamontowane 3 dyski twarde, każdy o pojemności 4TB znajdujące się na liście kompatybilności producenta oferowanego urządzenia NAS, spełniające wymagania: SATA 6 Gb/s, 3,5”, 64MB pamięci podręcznej, 5900 obr./min, MTBF min 1000000 h, czynnik drgań ruchu obrotowego, gwarancja producenta 3 lata	
Interfejsy sieciowe	2 porty 2,5Gigabit sieci Ethernet (RJ45)	
Porty	2 gniazda typu A USB 2.0 2 gniazda typu A USB 3.2 Gen 2 10 Gb/s 1 gniazdo HDMI 1.4b	
Porty PCIe	Co najmniej: 1x gniazdo Gen3 x2	
Wskaźniki LED	Dyski, stan, LAN, stan portów rozszerzenia pamięci masowej	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Obsługa RAID	RAID 0, 1, 5, 6, 10, 50, 60	
Funkcje RAID	Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD.	
Szyfrowanie	256-bitowe szyfrowanie AES folderów oraz szyfrowanie dysków zewnętrznych.	
System Operacyjny	Apple Mac OS 10.10 lub nowszy Linux and UNIX Microsoft Windows 7, 8, 10 i 11 Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016 I 2019	
Stacja monitoringu	Tak, w standardzie 8 darmowych licencji na podłączenie kamer.	
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, FC, Telnet, SSH, SNMP	
Usługi	Stacja monitoringu Windows ACL Integracja w Windows ADS Serwer WWW Serwer plików Manager plików przez WWW Funkcja Virtual Disk umożliwiaiąca zwiększenie pojemności serwera przy pomocy protokołu iSCSI Replikacja w czasie rzeczywistym Serwer RADIUS Klient LDAP Serwer Syslog Container Station	
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.	
Język GUI	Polski	
Gwarancja i serwis	36 miesięcy gwarancji producenta na macierz i dyski twarde	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Waga	Nie więcej niż 8 kg (netto)	
System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+	
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation	
Liczba kont użytkowników	4096	
Liczba grup	512	
Liczba udziałów	512	
Max ilość połączeń (CIFS)	1500	
Zasilanie	2x 300W, 100–240 V	
Wentylatory	2 x 80mm, 12VDC	
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.	
Lista funkcji które muszą być realizowane przez oprogramowanie do backupu:		
<ol style="list-style-type: none"> 1) Możliwość backupu stacji roboczych, serwerów, maszyn wirtualnych. 2) Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich 3) Program serwerowy kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10, Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019 Linux, BSD, Mac OS X 4) Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10, Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology 5) Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na 		

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

- poziomie fragmentów plików)
- 6) Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)
 - 7) Automatyczny backup przy wyłączeniu komputera (tylko Windows)
 - 8) Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych * i ?
 - 9) Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows)
 - 10) Backup baz danych i plików poczty w trybie online i offline
 - 11) Kopie rotacyjne (wersjonowanie)
 - 12) Zapis archiwów w otwartym formacie (ZIP 64-bit)
 - 13) Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi
 - 14) Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore)
 - 15) Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej
 - 16) Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych
 - 17) Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO
 - 18) Możliwość określenia liczby archiwów przechowywanych w miejscu replikacji (mniej lub więcej niż miejscu źródłowym)
 - 19) Kompresja po stronie stacji roboczej
 - 20) Replikacja archiwów (automatyczna lub według harmonogramu) na dodatkowy dysk twardy, NAS, serwer FTP,
 - 21) Centralne sterowanie całym Systemem z jednego miejsca
 - 22) Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników
 - 23) Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN
 - 24) Wysyłanie Alertów administracyjnych na e-mail
 - 25) Możliwość uruchamiania zewnętrznych

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

<p>programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych</p> <p>26) Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki</p> <p>27) Automatyczna aktualizacja oprogramowania na komputerach zdalnych</p> <p>28) Bezterminowa licencja - licencja nie może być ograniczona czasowo</p> <p>29) Interfejs, instrukcja i pomoc techniczna w języku polskim</p> <p>30) Rozmiar instalacji klienta < 1MB</p>	
<p>Usługa wdrożenia:</p>	
<p>Usługa wdrożenia powinna zostać zrealizowana zdalnie, a w jej zakresie powinny zawierać się przynajmniej:</p>	<ol style="list-style-type: none"> 1) Wysyłka przygotowanej do wdrożenia macierzy NAS (przeprowadzona integracja z oprogramowaniem do backupu), 2) Konfiguracja serwera backupu, 3) Przygotowanie paczki instalacyjnej aplikacji klienta backupu, 4) Omówienie i konfiguracja zadań backupu dla najważniejszych stacji klienckich, serwera oraz 4 hostów 5) Instruktażowe szkolenie administratora z wdrożonego systemu obejmujące przynajmniej omówienie konfiguracji i funkcji konsoli administracyjnej, procesu odzyskiwania danych oraz najlepszych praktyk dla rozwiązań backupowych.

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Tabela nr 6: Zestawienie parametrów technicznych oferowanego oprogramowania do monitorowania urządzeń Sieciowych*

L.p.	Nazwa parametru	Wartości minimalne wymagane przez Zamawiającego	Wartości oferowane przez Wykonawcę (tę kolumnę wypełnia Wykonawca) ⁷
1	2	3	4
			Proszę podać nazwę oferowanego oprogramowania:
1	Budowa oprogramowania	modułowa, składająca się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Moduły mają umożliwić kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomoc w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem.	
2	Zakres monitorowania infrastruktury	serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle przynajmniej w zakresie: 1) Serwisów TCP/IP, http, HTTPS, POP3, SMTP, IMAP, MAPI, FTP i innych wraz z możliwością definiowania	

⁷ Jeśli Wykonawca oferuje sprzęt w pełni odpowiadający wymaganiom opisanym w kol. „Wartości minimalne wymagane przez Zamawiającego”, wówczas w kol. „Wartości oferowane przez Wykonawcę” należy wpisać: „TAK”. Jeśli natomiast Wykonawca oferuje sprzęt o innych parametrach niż opisane w kol. „Wartości minimalne wymagane przez Zamawiającego”, wówczas w kol. „Wartości oferowane przez Wykonawcę” należy opisać wartości oferowane przez Wykonawcę.

*nie wskazanie terminu wykonania zamówienia będzie rozumiane że Wykonawca wskaże 60-dniowy termin wykonania.

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

		<p>własnych serwisów. System musi monitorować m.in. czas ich odpowiedzi i procent utraconych pakietów.</p> <p>2) Serwerów pocztowych:</p> <p>a) system musi monitorować zarówno serwis odbierający, jak i wysyłający pocztę,</p> <p>b) program musi mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdują się poza zakresem),</p> <p>c) program musi mieć możliwość wykonywania operacji testowych,</p> <p>d) program musi mieć możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa.</p> <p>3) Monitorowania serwerów WWW i adresów URL.</p> <p>4) Obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.</p> <p>5) Obsługi urządzeń SNMP wspierających SNMP v1/2/3 (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.).</p> <p>6) Obsługi komunikatów syslog</p>	
--	--	---	--

		<p>i pułapek SNMP.</p> <p>7) Monitoringu routerów i przełączników wg:</p> <p>a) zmian stanu interfejsów sieciowych,</p> <p>b) ruchu sieciowego,</p> <p>c) podłączonych stacji roboczych,</p> <p>d) ruchu generowanego przez podłączone stacje robocze.</p> <p>8) Serwisów Windows: monitor serwisów Windows musi alarmować gdy serwis przestanie działać oraz pozwalać na jego uruchomienie / zatrzymanie / zrestartowanie.</p> <p>9) Wydajności systemów Windows:</p> <p>a) obciążenie CPU,</p> <p>b) pamięci,</p> <p>c) zajętość dysków,</p> <p>d) transfer sieciowy.</p>	
3	Automatyczne definiowanie map urządzeń	<p>Zgodnie ze:</p> <p>1) zdefiniowaną przez administratora systemu strukturą organizacyjną</p> <p>2) zdefiniowanymi przez administratora filtrem; minimalne kryteria, które musi umożliwiać filtr:</p> <p>a) agent: stan, wersja, zainstalowany</p> <p>b) alarmy: aktywne</p> <p>c) aplikacje: zainstalowany program (zainstalowany lub nie), wersja aplikacji</p>	

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>(zainstalowana lub nie)</p> <p>d) usługi: monitorowane usługi, czas odpowiedzi</p> <p>e) SNMP: włączone, lokalizacja, mapowanie portów</p> <p>f) Właściwości urządzenia: rodzaj, nazwa, opis, adres MAC, adres IP.</p>	
4	<p>Moduł inwentaryzacji sprzętu sieciowego</p>	<p>Automatyczne gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych. Moduł powinien:</p> <ol style="list-style-type: none"> 1) Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp. 2) Informować o m.in.: zestawieniu posiadanych konfiguracji sprzętowych, wolnym miejscu na dyskach, średnim wykorzystaniu pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 3) Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwi audytowanie i weryfikację użytkownika licencji w organizacji. 4) Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: 	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

	<p>instalacji/deinstalacji aplikacji, zmian adresu IP itd.</p> <p>5) Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiegokolwiek zmiany konfiguracji sprzętowej komputera.</p> <p>6) Umożliwiać odczytanie numeru seryjnego (klucze licencyjne)</p> <p>Moduł inwentaryzacji sprzętu musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie:</p> <p>1) przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,</p> <p>2) definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania musi istnieć możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu</p>	
--	--	--

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

	<p>(musi być możliwość podania daty, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX), skan dowolnego dokumentu, czy też własny komentarz; dodatkowo musi być możliwość importu danych z zewnętrznego źródła (.CSV),</p> <p>3) generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania,</p> <p>4) archiwizacji i porównywania audytów środków trwałych,</p> <p>5) tworzenia kodów kreskowych w Środkach Trwałych,</p> <p>6) drukowania kodów kreskowych oraz QR Code (mozaikowe) dla środków trwałych, które posiadają numer inwentarzowy,</p> <p>7) inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej.</p> <p>Dostępne powinny być Agenty inwentaryzacji na systemy Android, OS X oraz Linux</p> <p>Inwentaryzacja oprogramowania</p>	
--	--	--

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:</p> <ol style="list-style-type: none"> 1) Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. 2) Zarządzanie posiadanymi licencjami. 3) Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili musi istnieć możliwość wykonania aktualnych raportów audytowych. 4) Zarządzanie posiadanymi licencjami: raport zgodności licencji. 5) Możliwość przypisania do programów numerów seryjnych, wartości itp. <p>Okna audytowe muszą posiadać możliwość filtrowania elementów z dokładnością do jednostki.</p>	
5	Moduł kontroli użytkowników	<p>Oprogramowanie musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez analizę:</p> <ol style="list-style-type: none"> 1) Faktycznego czasu aktywności (dokładny czas 	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

		<p>pracy z godziną rozpoczęcia i zakończenia pracy),</p> <ol style="list-style-type: none">2) Monitorowanie procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika),3) Rzeczywistego użytkownika programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona),4) Informacji o edytowanych przez użytkownika dokumentach,5) Historii pracy (cykliczne zrzuty ekranowe),6) Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),7) Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),8) Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości,
--	--	--

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,</p> <p>9) Nagłówków przesyłanej poczty e-mail.</p> <p>Oprogramowanie ponadto musi mieć funkcjonalność blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla danej stacji roboczej z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl).</p> <p>Oprogramowanie musi mieć możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.</p> <p>Oprogramowanie musi posiadać mechanizm blokowania uruchamiania aplikacji zdefiniowanej przez administratora.</p>	
6	Moduł pomocy zdalnej	Oprogramowanie musi umożliwiać realizację zdalnej pomocy użytkownikom.	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

		<p>W ramach kontroli stacji użytkownika musi być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator muszą widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu musi mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W module pomocy musi znajdować się baza zgłoszeń umożliwiającą użytkownikom zgłaszanie problemów technicznych, które z kolei muszą być przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. System musi umożliwiać użytkownikom monitorowanie procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które będą wpisywane i widoczne dla obu stron. Moduł ten musi również zawierać komunikator (czat), który musi umożliwiać przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i</p>	
--	--	--	--

		<p>administratorami. Moduł pomocy musi zawierać bazę wiedzy pomagającą użytkownikom na samodzielne rozwiązywanie najbardziej typowych problemów. Moduł pomocy zdalnej musi ponadto umożliwiać:</p> <ol style="list-style-type: none">1) pobieranie listy użytkowników z Active Directory,2) przypisywanie pracowników helpdesk do kategorii zgłoszeń,3) procesowanie zgłoszeń użytkowników z wiadomości e-mail,4) dołączanie załączników do zgłoszeń,5) zrzuty ekranowe (podgląd pulpitu),6) dystrybucję oprogramowania przez Agenty,7) dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),8) zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecenia operacji następuje kolejkowanie zadania dystrybucji pliku,9) możliwość skonfigurowania automatyzacji procesowania zgłoszeń,10) planowanie nieobecności pracowników helpdesk,11) generowanie raportów obsługi helpdesk.	
--	--	--	--

7	Moduł ochrony danych	<p>Oprogramowanie musi posiadać możliwość ochrony danych przed wyciekami poprzez blokowanie:</p> <ol style="list-style-type: none">1) urządzeń i nośników danych. System musi mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.2) urządzeń i interfejsów fizycznych: USB, FireWire, gniazd kart pamięci, dysków SATA, dysków przenośnych, napędów CD/DVD, stacji dyskietek.3) interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. <p>Blokownie musi dotyczyć tylko urządzeń służących do przenoszenia danych - inne urządzenia korzystające z tych interfejsów (drukarka, klawiatura, mysz itp.) muszą działać prawidłowo.</p> <p>Oprogramowanie musi zapewniać zarządzanie prawami dostępu do urządzeń:</p> <ol style="list-style-type: none">1) Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.	
---	-----------------------------	---	--

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>2) Autoryzowanie urządzeń firmowych (np. szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.</p> <p>3) Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników lub stacji roboczych.</p> <p>4) Centralną konfigurację poprzez ustawienie reguł (polityk) dla całej sieci lub wybranych stacji roboczych.</p>	
8	<p>Pozostałe parametry oprogramowania</p>	<p>Oprogramowanie musi zapewniać realizację audytu operacji na urządzeniach przenośnych:</p> <p>1) Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.</p> <p>2) Podłączenie/odłączenie urządzenia przenośnego.</p> <p>Oprogramowanie musi mieć możliwość integracji z usługą katalogową Active Directory w zakresie zarządzania prawami dostępu przypisanymi do użytkowników oraz grup domenowych.</p> <p>Agent na stacji roboczej musi być zabezpieczony przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora.</p> <p>Dostarczona licencja na</p>	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>oprogramowanie musi umożliwiać instalację dowolnej liczby serwerów zarządzania oraz konsoli zarządzających. Zamawiający musi mieć możliwość dowolnego przydziału licencji na każdy serwer zarządzania w ramach udzielonej licencji zbiorczej. Oprogramowanie musi być dostępny minimum w językach: polskim, angielskim, niemieckim.</p>	
10	Okres licencji	<p>Wieczysta licencja na oprogramowanie na 50 stanowisk z roczną aktualizacją do najnowszej wersji programu oraz rocznym dostępem do pomocy technicznej. Dostarczone oprogramowanie musi posiadać usługę wsparcia serwisowego realizowaną przez producenta oprogramowania przez okres nie krótszy niż 36 miesięcy od dnia dostarczenia licencji.</p>	

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Tabela nr 7: Zestawienie parametrów technicznych oferowanego urządzenia do ochrony brzegu sieci*

L.p.	Nazwa parametru	Wartości minimalne wymagane przez Zamawiającego	Wartości oferowane przez Wykonawcę (tę kolumnę wypełnia Wykonawca) ⁸
1	2	3	4
			Proszę podać producenta oraz typ/model oferowanego urządzenia:
1	Wymagania ogólne	1) Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi	

8 Jeśli Wykonawca oferuje sprzęt w pełni odpowiadający wymaganiom opisanym w kol. „Wartości minimalne wymagane przez Zamawiającego”, wówczas w kol. „Wartości oferowane przez Wykonawcę” należy wpisać: „TAK”. Jeśli natomiast Wykonawca oferuje sprzęt o innych parametrach niż opisane w kol. „Wartości minimalne wymagane przez Zamawiającego”, wówczas w kol. „Wartości oferowane przez Wykonawcę” należy opisać wartości oferowane przez Wykonawcę.

*nie wskazanie terminu wykonania zamówienia będzie rozumiane że Wykonawca wskaże 60-dniowy termin wykonania.

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

		<p>zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>2) System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>3) W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.</p> <p>4) System musi wspierać IPv4 oraz IPv6 w zakresie:</p> <ol style="list-style-type: none"> a) Firewall. b) Ochrony w warstwie aplikacji. c) Protokołów routingu dynamicznego. 	
2	<p>Redundancja, monitoring i wykrywanie awarii</p>	<p>1) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja</p>	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>synchronizacji sesji firewall.</p> <p>2) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.</p> <p>3) Monitoring stanu realizowanych połączeń VPN.</p> <p>4) ochrona przed spamem</p>	
3	Interfejsy, Dysk, Zasilanie	<p>1) System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45 w tym:</p> <p>a) min. 5 portów LAN</p> <p>b) min. 2 porty WAN</p> <p>c) min. 1 port DMZ</p> <p>2) System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</p> <p>3) W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.</p> <p>4) System musi być wyposażony w zasilanie AC.</p>	
4	Parametry wydajnościowe	<p>1) W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.</p> <p>2) Przepustowość Stateful Firewall: nie mniej niż 10 Gbps</p>	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>dla pakietów 512 B.</p> <p>3) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 600 Mbps.</p> <p>4) Wydajność szyfrowania IPsec VPN nie mniej niż 6 Gbps.</p> <p>5) Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.</p> <p>6) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.</p> <p>7) Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.</p>	
5	Funkcje Systemu Bezpieczeństwa	<p>W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <p>1) Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.</p> <p>2) Kontrola Aplikacji.</p> <p>3) Poufność transmisji danych - połączenia szyfrowane IPsec VPN oraz SSL VPN.</p> <p>4) Ochrona przed malware – co najmniej dla protokołów</p>	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

		<p>SMTP, POP3, IMAP, HTTP, FTP, HTTPS.</p> <ol style="list-style-type: none">5) Ochrona przed atakami - Intrusion Prevention System.6) Kontrola stron WWW.7) Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.8) Zarządzanie pasmem (QoS, Traffic shaping).9) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).10) Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.11) Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.12) Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym	
--	--	---	--

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		serwerze DNS jak i w ruchu przechodzącym przez system	
6	Polityki, Firewall	<ol style="list-style-type: none"> 1) Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2) System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: <ol style="list-style-type: none"> a) translację jeden do jeden oraz jeden do wielu. b) dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3) W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4) Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 5) Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. 	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>6) Amazon Web Services (AWS). 7) Microsoft Azure. 8) Google Cloud Platform (GCP). 9) OpenStack. 10)VMware NSX.</p>	
9	Połączenia VPN	<p>1) System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:</p> <ul style="list-style-type: none"> a) wsparcie dla IKE v1 oraz v2. b) obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). c) obsługa protokołu Diffie-Hellman grup 19 i 20. d) wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. e) tworzenie połączeń typu Site-to-Site oraz Client-to-Site. f) monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. g) możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. h) obsługa mechanizmów: IPSec NAT Traversal, DPD, 	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>Xauth.</p> <p>i) mechanizm „Split tunneling” dla połączeń Client-to-Site.</p> <p>2) System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:</p> <p>a) pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.</p> <p>b) pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.</p> <p>c) producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.</p>	
10	Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie powinno zapewniać obsługę:</p> <p>1) Routingu statycznego.</p> <p>2) Policy Based Routingu.</p> <p>3) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.</p>	
11	Funkcje SD-WAN	<p>1) System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia</p>	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>obciążenia do łączy WAN.</p> <p>2) Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.</p>	
12	Zarządzanie pasmem	<p>1) System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</p> <p>2) Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.</p> <p>3) System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.</p>	
13	Ochrona przed malware	<p>1) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>2) System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.</p> <p>3) System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</p> <p>4) System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w</p>	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.</p> <p>5) System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.</p> <p>6) Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</p>	
14	Ochrona przed atakami	<p>1) Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>2) System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.</p> <p>3) Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>4) Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>5) System musi zapewniać</p>	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p> <p>6) Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.</p> <p>7) Wykrywanie i blokowanie komunikacji C&C do sieci botnet.</p>	
15	Kontrola aplikacji	<p>1) Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>2) Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>3) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</p> <p>4) Baza powinna zawierać kategorie aplikacji szczególnie</p>	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>5) Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.</p>	
16	Kontrola WWW	<p>1) Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorii tematyczne.</p> <p>2) W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</p> <p>3) Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.</p> <p>4) Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>5) Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.</p> <p>6) Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł</p>	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

		<p>filtrowania.</p> <p>7) W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.</p>	
17	<p>Uwierzytelnianie użytkowników w ramach sesji</p>	<p>1) System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:</p> <ul style="list-style-type: none"> a) haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. b) haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. c) haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. <p>2) Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.</p> <p>3) Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.</p> <p>4) Uwierzytelnianie w oparciu o protokół SAML w politykach</p>	

		bezpieczeństwa systemu dotyczących ruchu HTTP.	
18	Zarządzanie	<ol style="list-style-type: none"> 1) Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2) Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3) Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego. 4) System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5) System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6) Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia 	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>7) Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p>	
19	Logowanie	<p>1) Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.</p> <p>2) W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p>	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		<p>3) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.</p> <p>4) Musi istnieć możliwość logowania do serwera SYSLOG.</p>	
20	Certyfikaty	<p>Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall.</p>	
21	Serwisy i licencje	<p>W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.</p>	
22	Gwarancja i wsparcie	<p>Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz</p>	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

		wsparcie techniczne w trybie 24x7.	
23	Rozszerzone wsparcie serwisowe AHB/SOS	<p>System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy. Oferent winien przedłożyć dokumenty:</p> <ol style="list-style-type: none"> 1) Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). 2) Certyfikat ISO 9001 podmiotu serwisującego. 	
24	Opisy do wymagań ogólnych	<ol style="list-style-type: none"> 1) W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały 	

Zadanie pn.: „Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

	<p>dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.</p> <p>2) Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.</p> <p>3) Urządzenie musi być fabrycznie nowe, wcześniej nie używane, dostarczone z wszystkimi standardowo oferowanymi przez producenta elementami i pochodzić z oficjalnego kanału sprzedaży.</p>	
--	---	--

3. **Deklarujemy termin wykonania przedmiotu umowy – Część nr 1*:** dodni od dnia zawarcia umowy (jeśli wykonawca pozostawi puste pole, Zamawiający przyjmie, że termin wykonania to 60 dni zgodnie z SWZ).
4. **Deklarujemy termin wykonania przedmiotu umowy – Część nr 2*:** dodni od dnia zawarcia umowy (jeśli wykonawca pozostawi puste pole, Zamawiający przyjmie, że termin wykonania to 60 dni zgodnie z SWZ).
5. **Deklarujemy termin wykonania przedmiotu umowy – Część nr 3*:** dodni od dnia zawarcia umowy (jeśli wykonawca pozostawi puste pole, Zamawiający przyjmie, że termin wykonania to 60 dni zgodnie z SWZ).
6. **Deklarujemy termin wykonania przedmiotu umowy – Część nr 4*:** dodni od dnia zawarcia umowy (jeśli wykonawca pozostawi puste pole, Zamawiający przyjmie, że termin wykonania to 60 dni zgodnie z SWZ).
7. **Deklarujemy termin wykonania przedmiotu umowy – Część nr 5*:** dodni od dnia zawarcia umowy (jeśli wykonawca pozostawi puste pole, Zamawiający przyjmie, że termin wykonania to 60 dni zgodnie z SWZ).
8. **Deklarujemy termin wykonania przedmiotu umowy – Część nr 6*:** dodni od dnia zawarcia umowy (jeśli wykonawca pozostawi puste pole, Zamawiający przyjmie, że termin wykonania to 60 dni zgodnie z SWZ).
9. **Deklarujemy termin wykonania przedmiotu umowy – Część nr 7*:** dodni od dnia zawarcia umowy (jeśli wykonawca pozostawi puste pole, Zamawiający przyjmie, że termin wykonania to 60 dni zgodnie z SWZ).
10. Warunki płatności – zgodnie ze wzorem umowy (załącznik nr 5 do SWZ).
11. Zamierzamy/nie zamierzamy powierzyć realizację następujących części zamówienia podwykonawcom*:

Lp.	Opis części zamówienia, którą Wykonawca zamierza powierzyć do realizacji przez Podwykonawcę	Nazwa Podwykonawcy

12. Płatności wynikające z realizacji ww. zadania prosimy przekazać na nasze konto numer(nr konta, nazwa banku).
13. OŚWIADCZAMY, że oferowane przez naszą Firmę prace są zgodne z wymaganiami Zamawiającego w tym zakresie określonym w SWZ.
14. 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⁾
15. Wyrażam dobrowolną zgodę na przetwarzanie dotyczących mnie danych osobowych

przez Administratora, którym jest Burmistrz Bierutowa, wykonujący zadania przy pomocy Urzędu Miejskiego w Bierutowie, zlokalizowanego w Bierutowie przy ul. Moniuszki 12, w zakresie - nazwa wykonawcy, imię, nazwisko, kraj, nip, adres: ulica, nr budynku, nr lokalu, kod pocztowy, miejscowość, nr rachunku bankowego, kwota wynagrodzenia, w celach niezbędnych do realizacji umowy o powierzenie grantu nr 2944/1/2021 z dnia 11.02.2022 r. oraz do badania kwalifikowalności środków, udzielenia wsparcia, ewaluacji, monitoringu, kontroli, sprawozdawczości, itp. w Projekcie realizowanym przez Miasto i Gminę Bierutów, pn.: „Cyfrowa Gmina”, który finansowany jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, w ramach konkursu grantowego Cyfrowa Gmina o numerze POPC.05.01.00-00-0001/21-00.

16. **INFORMUJEMY**, że jesteśmy:

- mikroprzedsiębiorstwem / małym przedsiębiorstwem / średnim przedsiębiorstwem*
- dużym przedsiębiorstwem*

17. **OŚWIADCZAMY**, że zapoznaliśmy się ze Specyfikacją Warunków Zamówienia i nie wnosimy do niej zastrzeżeń. **OŚWIADCZAMY**, że otrzymaliśmy konieczne informacje potrzebne do właściwego przygotowania oferty.

18. **OŚWIADCZAMY**, że zapoznaliśmy się z Projektowanymi Postanowieniami Umowy, określonymi w Załączniku nr 5 do Specyfikacji Warunków Zamówienia i **ZOBOWIĄZUJEMY SIĘ**, w przypadku wyboru naszej oferty, do zawarcia umowy zgodnej z niniejszą ofertą, na warunkach w nich określonych.

19. **OŚWIADCZAMY**, że uważamy się za związanych złożoną ofertą na okres 30 dni od dnia, w którym upływa termin składania ofert.

20. **OŚWIADCZAMY**, że osobą do kontaktów i dokonywania bieżących ustaleń z Zamawiającym jest:

L.p.	Imię i Nazwisko	Telefon

21. Zostaliśmy poinformowani, że możemy wydzielić z oferty informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i zastrzec w odniesieniu do tych informacji, aby nie były one udostępnione.

22. Wraz z ofertą **SKŁADAMY** następujące oświadczenia i dokumenty:

L.p.	Nazwa załącznika
1	
2	

Informacja dla Wykonawcy:

- 1. Formularz oferty musi być opatrzony przez osobę lub osoby uprawnione do reprezentowania firmy kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub elektronicznym podpisem osobistym i przekazany Zamawiającemu wraz z dokumentem (-ami) potwierdzającymi prawo do reprezentacji Wykonawcy przez osobę podpisującą ofertę.**
- W celu potwierdzenia, że osoba działająca w imieniu wykonawcy jest umocowana do jego reprezentowania, Wykonawca przedkłada odpis lub informację z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru.
- Wykonawca nie jest zobowiązany do złożenia dokumentów, o których mowa w pkt 1, jeżeli Zamawiający może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, o ile wykonawca wskazał dane umożliwiające dostęp do tych dokumentów.
- Jeżeli w imieniu Wykonawcy działa osoba, której umocowanie do jego reprezentowania nie wynika z dokumentów, o których mowa w pkt 2, Wykonawca wraz z ofertą składa pełnomocnictwo lub inny dokument potwierdzający umocowanie do reprezentowania Wykonawcy.
- Przepis pkt 4 stosuje się odpowiednio do osoby działającej w imieniu wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego.
- Przepisy pkt 2–4 stosuje się odpowiednio do osoby działającej w imieniu podmiotu udostępniającego zasoby na zasadach określonych w art. 118 ustawy lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach.
- W przypadku wskazania przez Wykonawcę dostępności podmiotowych środków dowodowych lub dokumentów, o których mowa w pkt 2, pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych, Zamawiający może żądać od Wykonawcy przedstawienia tłumaczenia na język polski pobranych samodzielnie przez zamawiającego podmiotowych środków dowodowych lub dokumentów.

8. Wykonawca podpisując niniejszą ofertę oświadcza jednocześnie, że zapoznał się z Klauzulą informacyjną RODO oraz wyraża zgodę na udostępnienie i przetwarzanie danych osobowych zgodnie z załącznikiem nr 9.

* niepotrzebne skreślić

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), zwana RODO.

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).

**Załącznik Nr 2 – do SWZ
Oświadczenie wykonawcy**

Nazwa zadania:

Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” Część nr 1*/ Część nr 2*/Część nr 3*/Część nr 4*/Część nr 5*/Część nr 6*/Część nr 7*

Nazwa Wykonawcy	Adres Wykonawcy

Oświadczenia Wykonawcy*/Wykonawcy wspólnie ubiegającego się o udzielenie zamówienia*

UWZGLĘDNIAJĄCE PRZESŁANKI WYKLUCZENIA Z ART. 7 UST. 1 USTAWY O SZCZEGÓLNYCH ROZWIĄZANIACH W ZAKRESIE PRZECIWDZIAŁANIA WSPIERANIU AGRESJI NA UKRAINĘ ORAZ SŁUŻĄCYCH OCHRONIE BEZPIECZEŃSTWA NARODOWEGO

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (dalej jako: Pzp)

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”**, prowadzonego przez Miasto i Gminę Bierutów, oświadczam, co następuje:

OŚWIADCZENIE DOTYCZĄCE PODSTAW WYKLUCZENIA:

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy Pzp.
2. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 109 ust. 1 pkt 4, 5, 7 ustawy Pzp.
3. Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ustawy Pzp (podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2 i 5 lub art. 109 ust. 1 pkt 2-5 i 7-10 ustawy Pzp). Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjąłem następujące środki naprawcze i zapobiegawcze:

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

-
4. Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. poz. 835)⁹.

OŚWIADCZENIE DOTYCZĄCE WARUNKÓW UDZIAŁU W POSTĘPOWANIU:

Oświadczam, że spełniam, określone przez Zamawiającego, warunki udziału w postępowaniu w zakresie:

- 1) zdolności do występowania w obrocie gospodarczym;
- 2) uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów;
- 3) sytuacji ekonomicznej lub finansowej;
- 4) zdolności technicznej lub zawodowej.

INFORMACJA W ZWIĄZKU Z POLEGANIEM NA ZDOLNOŚCIACH LUB SYTUACJI PODMIOTÓW UDOSTĘPNIAJĄCYCH ZASOBY (JEŚLI DOTYCZY):

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez Zamawiającego w.....

9 Zgodnie z treścią art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, zwanej dalej „ustawą”, z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:

- 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 ustawy;
- 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 ustawy;
- 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 ustawy.

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

..... (wskazać dokument i właściwą jednostkę redakcyjną dokumentu, w której określono warunki udziału w postępowaniu), polegam na zdolnościach lub sytuacji następującego/yh podmiotu/ów udostępniających zasoby: (wskazać nazwę/y podmiotu/ów)
..... w następującym zakresie:
(określić odpowiedni zakres udostępnianych zasobów dla wskazanego podmiotu).

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

INFORMACJA DOTYCZĄCA DOSTĘPU DO PODMIOTOWYCH ŚRODKÓW DOWODOWYCH:

Wskazuję następujące podmiotowe środki dowodowe, które można uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, oraz dane umożliwiające dostęp do tych środków:

- 1)
..... (wskazać podmiotowy środek dowodowy, adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji)
- 2)
..... (wskazać podmiotowy środek dowodowy, adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji)

*niepotrzebne skreślić

Informacja dla Wykonawcy:

- 1) Podpisuje każdy wykonawca składający ofertę
- 2) W przypadku Wykonawców wspólnie ubiegających się o zamówienie powyższy dokument podpisują wszyscy członkowie konsorcjum lub Pełnomocnik w imieniu całego konsorcjum.
- 3) **Dokument musi być opatrzony przez osobę lub osoby uprawnione do reprezentowania firmy kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub elektronicznym podpisem osobistym.**

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

- 4) Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych, jeżeli może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile wykonawca wskazał w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy Pzp, dane umożliwiające dostęp do tych środków.
- 5) Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które Zamawiający posiada, jeżeli Wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.

Załącznik Nr 3 – do SWZ
Oświadczenie podmiotu udostępniającego zasoby (jeśli dotyczy)

Nazwa zadania:

Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” Część nr 1*/ Część nr 2*/Część nr 3*/Część nr 4*/Część nr 5*/Część nr 6*/Część nr 7*

Nazwa Wykonawcy	Adres Wykonawcy

**Oświadczenia podmiotu udostępniającego zasoby
UWZGLĘDNIAJĄCE PRZESŁANKI WYKLUCZENIA Z ART. 7 UST. 1 USTAWY O
SZCZEGÓLNYCH ROZWIĄZANIACH W ZAKRESIE PRZECIWDZIAŁANIA
WSPIERANIU AGRESJI NA UKRAINĘ ORAZ SŁUŻĄCYCH OCHRONIE
BEZPIECZEŃSTWA NARODOWEGO
składane na podstawie art. 125 ust. 5 ustawy Pzp**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”**, prowadzonego przez Miasto i Gminę Bierutów, oświadczam, co następuje:

OŚWIADCZENIE DOTYCZĄCE PODSTAW WYKLUCZENIA:

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy Pzp.
2. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 109 ust. 1 pkt 4, 5, 7 ustawy Pzp.
3. Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. poz. 835)¹⁰.

¹⁰ Zgodnie z treścią art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

OŚWIADCZENIE DOTYCZĄCE WARUNKÓW UDZIAŁU W POSTĘPOWANIU:

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez Zamawiającego w
..... (wskazać dokument i właściwą jednostkę redakcyjną dokumentu, w której określono warunki udziału w postępowaniu) w następującym zakresie:.....

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

INFORMACJA DOTYCZĄCA DOSTĘPU DO PODMIOTOWYCH ŚRODKÓW DOWODOWYCH:

Wskazuję następujące podmiotowe środki dowodowe, które można uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, oraz dane umożliwiające dostęp do tych środków:

- 1)
..... (wskazać podmiotowy środek dowodowy, adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji)

narodowego, zwanej dalej „ustawą”, z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:

- 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 ustawy;
- 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 ustawy;
- 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 ustawy.

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

- 2)
..... (wskazać podmiotowy środek dowodowy, adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji)

*niepotrzebne skreślić

Informacja dla Wykonawcy:

- 1) Podpisuje każdy wykonawca składający ofertę
- 2) W przypadku Wykonawców wspólnie ubiegających się o zamówienie powyższy dokument podpisują wszyscy członkowie konsorcjum lub Pełnomocnik w imieniu całego konsorcjum.
- 3) **Dokument musi być opatrzony przez osobę lub osoby uprawnione do reprezentowania firmy kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub elektronicznym podpisem osobistym.**
- 4) Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych, jeżeli może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile wykonawca wskazał w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy Pzp, dane umożliwiające dostęp do tych środków.
- 5) Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które Zamawiający posiada, jeżeli Wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Załącznik Nr 4a – do SWZ
Opis przedmiotu zamówienia – część nr 1

Nazwa zadania:

Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”

Nazwa Wykonawcy	Adres Wykonawcy

Część nr 1 – Zakup serwerów
Specyfikacja techniczna/formularz do wypełnienia przez Wykonawcę

Nazwa komponentu	Wymagane parametry minimalne	Potwierdzenie spełnienia wymagań (Należy wpisać SPEŁNIA oraz podać istotne parametry faktyczne)*
Typ	Serwer – 2 szt.	Producent: Model:
Procesor	Zainstalowany jeden procesor sześciordzeniowy dedykowany do pracy z zaofertowanym serwerem, taktowany zegarem min 2.9 GHz (częstotliwość bazowa) umożliwiający osiągnięcie wyniku minimum 16 600 punktów w teście PassMark - CPU Mark dostępnym na stronie internetowej https://www.cpubenchmark.net/high_end_cpus.html z dnia 01.06.2022 r.	Producent: Model:

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Płyta główna	Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.	Producent:
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych	Należy podać typ procesora:
Obudowa	Obudowa Rack 19" o wysokości max 1U z możliwością instalacji 8 dysków 2,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.	
RAM	64 GB pamięci RAM ECC UDIMM w kościach 32GB o częstotliwości pracy 3200MT/s. Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci	Zainstalowana pamięć RAM: Obsługiwana pamięć RAM:
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200	
Gniazda PCI	Min. 2 sloty PCIe generacji 4	
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)	
Wbudowane porty	min. 4 porty USB w tym min. 1 port USB 3.0 z tyłu obudowy, 1 port VGA na tylnym panelu, min. 1 port RS232	

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00



Kontroler dysków	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfujących.	
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD, NL SAS Zainstalowane 2 dyski SSD SATA o pojemności min. 960GB, 6Gb, Hot-Plug o parametrze DWPD wynoszącym min. 1. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.	
System diagnostyczny	Diody LED informujące o kondycji serwera.	
Wentylatory	Minimum 4 wentylatory	
Zasilacze	Dwa zasilacze o mocy min. 600W	
System operacyjny/ dodatkowe oprogramowanie	Zainstalowany fabrycznie Windows Serwer w wersji 2022 Standard	



<p>Bezpieczeństwo</p>	<ol style="list-style-type: none"> 1) Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardej. 2) Możliwość wyłączenia w BIOS funkcji przycisku zasilania. 3) Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. 4) Moduł TPM 2.0 5) Możliwość dynamicznego włączania i wyłączenia portów USB na obudowie – bez potrzeby restartu serwera 6) Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem 	
<p>Diagnostyka</p>	<p>Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.</p>	
<p>Karta Zarządzania</p>	<ol style="list-style-type: none"> 1) Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: 2) zdalny dostęp do graficznego interfejsu Web karty zarządzającej; 3) zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji 	



	<p>serwera);</p> <ol style="list-style-type: none"> 4) szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; 5) wsparcie dla IPv6; 6) wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; 7) możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; 8) integracja z Active Directory; 9) wsparcie dla dynamic DNS; 10) wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. 11) możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera. 12) możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera 	
<p>Gwarancja</p>	<p>min.5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk</p>	



	<p>twardy pozostaje u Zamawiającego.</p> <p>Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.</p> <p>Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p> <p>Możliwość rozszerzenia gwarancji przez producenta do 7 lat.</p> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera</p>	
Dokumentacja	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>	
Dodatkowe informacje	<p>Urządzenie musi być fabrycznie nowe, wcześniej nie używane, z wszystkimi standardowo dołączanymi przez producenta elementami oraz pochodzić z oficjalnego kanału sprzedaży.</p>	



Fundusze
Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

UWAGA:

Wypełnioną i podpisaną tabelę należy złożyć wraz z ofertą.

***Prawą stroną tabeli należy wypełnić stosując słowa „spełnia” lub „nie spełnia”, zaś w przypadku żądania wykazania wpisu określonych parametrów, należy wpisać oferowane konkretne, rzeczowe wartości. W przypadku, gdy Wykonawca, w którejkolwiek z pozycji wpisze słowa „nie spełnia” lub zaoferuje niższe wartości, oferta zostanie odrzucona, gdyż jej treść nie odpowiada treści SWZ**

(Oświadczenie musi być opatrzone przez osobę lub osoby uprawnione do reprezentowania Wykonawcy kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym)



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Załącznik Nr 4b – do SWZ
Opis przedmiotu zamówienia – część nr 2

Nazwa zadania:

Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”

Nazwa Wykonawcy	Adres Wykonawcy

Część nr 2 – Modernizacja wewnętrznej sieci LAN
Specyfikacja techniczna/formularz do wypełnienia przez Wykonawcę

Nazwa komponentu	Wymagane parametry minimalne	Potwierdzenie spełnienia wymagań (Należy wpisać SPEŁNIA oraz podać istotne parametry faktyczne)*
Ilość punktów elektryczno-logicznych (PEL)	50 PEL (Szczegółowa lokalizacja PEL zostanie wskazana na etapie opracowania projektu wykonawczego.)	
Elementy składowe każdego punktu elektryczno-logicznego (PEL)	1) dwa gniazda RJ45 (montowane w kanałach instalacyjnych natynkowych) kategorii 6a lub wyższej oraz 2) dwa gniazda elektryczne 230V (montowane w korycie) z blokadą uniemożliwiającą podłączenie nieuprawnionych odbiorników.	

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00



<p>Wymagania dotyczące dostarczonej szafy serwerowej</p>	<p>3) Wysokość 37U (max 1800 mm), 4) Szerokość nie mniej niż 600x800 mm, 5) Wyposażenie szafy: a) panel wentylacyjny, b) panele krosowe modułarne kat.6, c) panele z przewodnikami kabla w ilości równej panelom krosowniczym, d) 2 listwy zasilające, e) 2 półki o głębokości min 600 mm i obciążalności min 80 kg, 6) Konfiguracja szafy: a) standardowo wyposażona przez producenta w drzwi przednie oszklone z możliwością zmiany strony mocowania, b) zdejmowane osłony boczne, c) możliwość wyprowadzenia kabli przez podłogę sufit oraz tył szafy, d) profile montażowe regulowane, e) inne, standardowe dołączane przez producenta wyposażenie.</p>	
<p>Prace przewidziane w ramach instalacji okablowania strukturalnego</p>	<p>1) budowa nowych tras kablowych, 2) układanie kabli w nowych i istniejących trasach, 3) instalacja punktów PEL - (punkt elektryczno-logiczny), 4) montaż paneli krosowych 48xRJ45 w szafie serwerowej i</p>	



	<p>ewentualnych szafach dystrybucyjnych,</p> <p>5) dostarczenie i montaż szafy serwerowej i ewentualnych szaf dystrybucyjnych oraz patchpaneli krosowych RJ45 kat. 6; ilość paneli należy dostosować do liczby instalowanych gniazd z zapewnieniem 50% nadmiarowości,</p> <p>6) terminowanie kabli w osprzęcie przyłączeniowym,</p> <p>7) pomiary tras kablowych, wykonanie dokumentacji powykonawczej.</p>	
<p>Wymagane parametry funkcjonalno-użytkowe okablowania strukturalnego</p>	<p>1)system okablowania strukturalnego co najmniej kategorii 6a musi zapewnić możliwość transmisji głosu, danych, sygnałów wideo,</p> <p>2)w okablowaniu muszą być zastosowane 4-parowe kable symetryczne UTP, które charakteryzują się parametrami i jakością niezbędną do prawidłowej pracy systemu zarówno w chwili obecnej, jak i w przyszłości,</p> <p>3)budowane trasy mają być prowadzone w kanale instalacyjnym natynkowym (korytka PCV),</p> <p>4)izolacja zewnętrzna okablowania miedzianego musi być wykonana z PVC lub z materiału LSZH nie wydzielającego toksycznych oparów podczas spalania (nie zawiera halogenu),</p> <p>5)w okablowaniu wszystkie komponenty (w tym parametry transmisyjne) muszą charakteryzować się pełną zgodnością ze specyfikacją dla kategorii 6,</p>	



	<p>6) moduły RJ45 powinny być zarabiane narzędziowo, 7) gniazda naścienne i na panelu krosowym muszą być oznaczone tj. posiadać czytelną numerację na obydwu końcach toru, 8) wymiar panelu krosowego musi być następujący - szerokość 19", max wysokość 2 U, 9) panel musi umożliwić zamontowanie min. 24 modułów RJ45, okablowanie musi bazować na jednorodnym rozwiązaniu systemu okablowania strukturalnego, którego wszystkie elementy toru transmisyjnego pochodzą od tego samego producenta.</p>	
<p>Wymagania dotyczące wykonania dedykowanej instalacji elektrycznej</p>	<p>1) rozbudowa instalacji elektrycznej gniazd wtykowych zasilania dedykowanego – dwa gniazda na PEL, 2) rozbudowa istniejących rozdzielnic lub ich wymiany (w przypadku braku możliwości rozbudowy), 3) wykonania dedykowanej instalacji zasilającej w układzie TN-S, 4) wszystkie gniazda elektrycznej sieci zasilającej, powinny posiadać zabezpieczenie w postaci klucza typu DATA, aby uniemożliwić podłączenia dowolnych urządzeń elektrycznych i tym samym wprowadzić podniesienie bezpieczeństwa użytkownika. Wymagane jest dostarczenie kluczy w ilości odpowiadającej zainstalowanym gniazdom,</p>	



- 5) do budowy toru zasilającego koniecznym jest użycie przewodów izolowanych YDY – 750V, 3x2,5 mm² lub innych o porównywalnych parametrach izolacyjno-eksploatacyjnych,
- 6) obwody elektryczne w obrębie pomieszczeń mają być prowadzone łącznie z instalacją logiczną w kanale instalacyjnym natynkowym (korytka PCV) - rozdzielone przegrodą lub w odrębnych kanałach,
- 7) należy zaprojektować max. 5 urządzeń na jeden obwód zabezpieczający,
- 8) każdy obwód elektryczny musi zostać zabezpieczony wyłącznikiem przepięciowym i różnicowo-prądowym.

Instalację należy zasilić z dedykowanej rozdzielni głównej budynku.

Od istniejących tablic rozdzielczych zostanie wykonane zasilanie YDY-żo 5x10mm.

Do instalacji zostanie zamontowany podlicznik energii elektrycznej.

Dla poprawienia wartości uziomu, który nie powinien przekraczać wartości 10Ω, jeżeli zajdzie taka potrzeba, zostanie wbity pręty pomiedziowane typu galmar, w okolicy istniejącego złącza kablowego na zewnątrz budynku, aby zapewnić prawidłowe funkcjonowanie ochrony TN-S w całym



	<p>obiekcie.</p> <p>W istniejących tablicach elektrycznych zostaną umieszczone zabezpieczenia gniazd zasilania komputerowego.</p> <p>Szafa serwerowa będzie podłączona do osobnego zabezpieczenia przepięciowego i różnicowo-prądowego. W przypadku, gdy istniejące tablice okażą się za małe, zostaną wymienione na nowe.</p> <p>Instalacja gniazd wtyczkowych zostanie wykonana przewodami miedzianymi typu YDY-żo 3x750V o przekroju 2,5 mm. z osobną żyłą „N” i PE. Wszystkie gniazda wtyczkowe będą posiadać bolec ochronny.</p> <p>Obwód gniazd komputerowych 230V, w tablicach elektrycznych zostanie zabezpieczony wyłącznikiem różnicowo-prądowym 16A, $\Delta I=0,03A$, o charakterystyce typu „A”.</p> <p>Jako dodatkową ochronę od porażień prądem elektrycznym po stronie nn-0,4kV zastosowane zostaną „samoczynne wyłączanie zasilania” w układzie TN-C-S (dla sieci zasilającej układ TN-C, dla odbiorczej TN-S). W celu zapewnienia ochrony przepięciowej, zastosowane zostaną odgromniki 4xDEHNbloc i ochronniki przepięciowe 4xDEHNquard. Dla prawidłowego funkcjonowania ochrony przepięciowej zastosowany zostanie dławiki typu DEHNbridge.</p>	
--	--	--



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Gwarancja	min. 5 lat na wykonaną instalację oraz dostarczony sprzęt.	
Dodatkowe informacje	Elementy PEL (punktów elektryczno-logicznych) oraz szafy serwerowej muszą być fabrycznie nowe, wcześniej nie używane, dostarczone z wszystkimi standardowo dołączanymi przez producenta elementami.	

UWAGA:

Wypełnioną i podpisaną tabelę należy złożyć wraz z ofertą.

***Prawą stroną tabeli należy wypełnić stosując słowa „spełnia” lub „nie spełnia”, zaś w przypadku żądania wykazania wpisu określonych parametrów, należy wpisać oferowane konkretne, rzeczowe wartości. W przypadku, gdy Wykonawca, w którejkolwiek z pozycji wpisze słowa „nie spełnia” lub zaoferuje niższe wartości, oferta zostanie odrzucona, gdyż jej treść nie odpowiada treści SWZ**

(Oświadczenie musi być opatrzone przez osobę lub osoby uprawnione do reprezentowania Wykonawcy kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym)



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Załącznik Nr 4c – do SWZ
Opis przedmiotu zamówienia – część nr 3

Nazwa zadania:

Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”

Nazwa Wykonawcy	Adres Wykonawcy

**Część nr 3 – Zakup urządzenia wielofunkcyjnego z możliwością skanowania do sieci
Specyfikacja techniczna/formularz do wypełnienia przez Wykonawcę**

Nazwa komponentu	Wymagane parametry minimalne	Potwierdzenie spełnienia wymagań (Należy wpisać SPEŁNIA oraz podać istotne parametry faktyczne)*
Typ	Urządzenie wielofunkcyjne	Producent: Model:
Technologia druku	technologia laserowa	
Format skanowanego oryginału	A3	
Format kopii	A3-A6	
Prędkość drukowania	A4	nie mniej niż 26 stron/min.
	A3	nie mniej niż 15 stron/min.

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Obsługiwane rozdzielczości drukowania	Nie gorsza niż 1200x600 dpi oraz 600x600 dpi	
Czas wydruku pierwszej strony	maks. 5 sek.	
Czas nagrzewania	maks. 20 sek. od włączenia zasilania	
Kopiowanie wielokrotne	do 999 kopii	
Pamięć RAM	min. 2 GB	
Dysk HDD lub SSD	min. 30 GB	
Zoom	25-400%	
Panel operatora	Panel wyposażony w kolorowy ekran dotykowy LCD, min. 7-calowy, opisy na panelu oraz komunikaty na ekranie w języku polskim.	
Dupleks	Automatyczny, obsługa papieru 60-160 g/m ²	
Podajnik dokumentów	Automatyczny dwustronny, taca podającej na min. 140 ark. 80 g/m ²	
Podajnik papieru	podajnik o pojemności min. 2 x 500 ark. A5-A3 (80 g/m ²), 60-160 g/m ² taca boczna, min. 100 ark. A6-A3 (80 g/m ²), 60-250 g/m ²	
Odbiornik wydruków i kopii	Taca odbiorcza na min. 250 ark. (80 g/m ²)	

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Podstawa na kółkach	Dedykowana podstawa producenta urządzenia z katalogu dostępnych fabrycznie opcji, zamykana, na kółkach. Dopasowana kolorystycznie, wzorniczo i kształtem do obudowy urządzenia.	
Pamięć drukarki	Współdzielona z kopiarką (dotyczy pamięci RAM i dysku)	
Emulacje	PCL 6, PostScript Level 3	
Interfejsy	USB 2.0, Ethernet 10/100/1000Base-T	
Funkcje skanowania	skanowanie do PC, do e-mail, do FTP, sieciowy TWAIN, do pamięci przenośnej USB, WIA, SMB, do skrzynki dokumentów	
Rozdzielczość skanowania	600 dpi lub lepsza	
Prędkość skanowania	min. 80 str. / min. (A4, kolor, 300 dpi)	
Typy plików	PDF, JPEG, TIFF, XPS, PDF szyfrowany, PDF/A	
Materiały eksploatacyjne jako wyposażenie standardowe (dostarczone w komplecie w ramach oferowanej ceny)	Tonery: w ilości, która zapewni wydrukowanie minimum 20 000 stron A4 (zgodnie z ISO 19752) Bębny: w ilości, która zapewni wydrukowanie minimum 600 000 stron A4. Dostarczone materiały muszą być nowe, nieregenerowane i wyprodukowane przez producenta oferowanych urządzeń.	

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00



jednostkowej).		
Możliwość rozbudowy	<p>1) Podajnik papieru na min. 3000 ark. A4, 80 g/m²;</p> <p>2) finiszier zszywający, min. 2 tace odbiorcze o łącznej pojemności min. 3.000 ark. A4-80 g/m², obsługa papieru o wadze 60-250 g/m² ,</p> <p>3) zszywacz min. 50 ark., dziurkacz 2/4;</p>	
Funkcja dodatkowa	Urządzenie wyposażone w funkcję zgłaszania usterek bezpośrednio z panelu dotykowego urządzenia.	
Wymagania dodatkowe	Oferent musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzenia wielofunkcyjnego - dokumenty potwierdzające dołączyć do oferty	
	Certyfikat ISO 9001:2015 producenta oferowanego sprzętu - dokument potwierdzający załączyć do oferty	
	Certyfikat ISO 14001:2015 producenta oferowanego sprzętu - dokument potwierdzający załączyć do oferty	
	Oświadczenie producenta oferowanego sprzętu lub jego autoryzowanego przedstawiciela w Polsce, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Konieczność nie zachodzi w przypadku autoryzowanego przedstawiciela producenta.	



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

	Urządzenie musi być fabrycznie nowe, wcześniej nie używane, dostarczone z wszystkimi standardowo oferowanymi przez producenta elementami i pochodzić z oficjalnego kanału sprzedaży.	
Gwarancja	Gwarancja producenta nie mniej niż 24 miesięcy	

UWAGA:

Wypełnioną i podpisaną tabelę należy złożyć wraz z ofertą.

***Prawą stroną tabeli należy wypełnić stosując słowa „spełnia” lub „nie spełnia”, zaś w przypadku żądania wykazania wpisu określonych parametrów, należy wpisać oferowane konkretne, rzeczowe wartości. W przypadku, gdy Wykonawca, w którejkolwiek z pozycji wpisze słowa „nie spełnia” lub zaoferuje niższe wartości, oferta zostanie odrzucona, gdyż jej treść nie odpowiada treści SWZ**

(Oświadczenie musi być opatrzone przez osobę lub osoby uprawnione do reprezentowania Wykonawcy kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym)



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Załącznik Nr 4d – do SWZ
Opis przedmiotu zamówienia – część nr 4

Nazwa zadania:

Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”

Nazwa Wykonawcy	Adres Wykonawcy

Część nr 4 – Zakup oprogramowania biurowego
Specyfikacja techniczna/formularz do wypełnienia przez Wykonawcę

Nazwa komponentu	Wymagane parametry minimalne	Potwierdzenie spełnienia wymagań (Należy wpisać SPEŁNIA oraz podać istotne parametry faktyczne)*
Oprogramowanie biurowe (50 stanowisk)	Oprogramowanie biurowe Microsoft 365 Business Basic.	
Oprogramowanie biurowe (40 stanowisk)	Oprogramowanie biurowe Microsoft 365 Business Standard.	
Zastosowanie	Dla jednostek administracji samorządowej	
Okres licencji	18 miesięcy	
Wersja językowa	Polska	

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00



Fundusze
Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

UWAGA:

Wypełnioną i podpisaną tabelę należy złożyć wraz z ofertą.

***Prawą stroną tabeli należy wypełnić stosując słowa „spełnia” lub „nie spełnia”, zaś w przypadku żądania wykazania wpisu określonych parametrów, należy wpisać oferowane konkretne, rzeczowe wartości. W przypadku, gdy Wykonawca, w którejkolwiek z pozycji wpisze słowa „nie spełnia” lub zaoferuje niższe wartości, oferta zostanie odrzucona, gdyż jej treść nie odpowiada treści SWZ**

(Oświadczenie musi być opatrzone przez osobę lub osoby uprawnione do reprezentowania Wykonawcy kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym)



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Załącznik Nr 4e – do SWZ
Opis przedmiotu zamówienia – część nr 5

Nazwa zadania:

Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”

Nazwa Wykonawcy	Adres Wykonawcy

**Część nr 5 – Zakup systemu do tworzenia kopii bezpieczeństwa
Specyfikacja techniczna/formularz do wypełnienia przez Wykonawcę**

Nazwa komponentu	Wymagane parametry minimalne	Potwierdzenie spełnienia wymagań (Należy wpisać SPEŁNIA oraz podać istotne parametry faktyczne)*
Opis ogólny	<p>Kompleksowe, zintegrowane rozwiązanie do backupu wraz z usługą wdrożenia zdalnego oraz pomocą techniczną wykonawcy na okres 1 roku.</p> <p>W zastosowanym rozwiązaniu oprogramowanie do centralnego zarządzania backupem ma być zintegrowane z platformą sprzętową serwera NAS tak aby nie było potrzeby instalacji serwera backupu (serwera zarządzania) na osobnym serwerze klienta.</p>	<p>Producent i model platformy sprzętowej:</p> <p>.....</p> <p>Producent nazwa oprogramowania</p> <p>.....</p>

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

	<p>System powinien umożliwić archiwizację 40 stacji roboczych 2 serwery (Windows Server) oraz 4 hosty Hyper-V.</p> <p>Zamawiający wymaga dostarczenia i wdrożenia rozwiązania składającego się z urządzenia NAS, dysków twardych oraz oprogramowania do backupu spełniających poniższe wymagania.</p>	
Minimalna specyfikacja platformy sprzętowej:		
Procesor	<p>Jeden 4-rdzeniowy/4-wątkowy Intel Celeron N5105/N5095 lub równoważny procesor osiągający w testach PassMark - CPU Mark wynik nie gorszy niż 4000 pkt.</p> <p>W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie https://www.cpubenchmark.net</p>	
Obudowa	Rack 2U o wymiarach nie większych niż, 87× 483 × 347 mm (wys. x szer. x gł.); w zestawie szyny wysuwane do instalacji w szafie RACK	
Pamięć RAM	4 GB SODIMM DDR4 Urządzenie powinno obsługiwać do 16GB pamięci RAM.	
Ilość obsługiwanych dysków	8 dysków 3,5-calowych 3,5/2,5 dyski SATA	
Zamontowane dyski twarde	Zamontowane 3 dyski twarde, każdy o pojemności 4TB znajdujące się na liście kompatybilności producenta	

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00



	oferowanego urządzenia NAS, spełniające wymagania: SATA 6 Gb/s, 3,5”, 64MB pamięci podręcznej, 5900 obr./min, MTBF min 1000000 h, czynnik drgań ruchu obrotowego, gwarancja producenta 3 lata	
Interfejsy sieciowe	2 porty 2,5Gigabit sieci Ethernet (RJ45)	
Porty	2 gniazda typu A USB 2.0 2 gniazda typu A USB 3.2 Gen 2 10 Gb/s 1 gniazdo HDMI 1.4b	
Porty PCIe	Co najmniej: 1x gniazdo Gen3 x2	
Wskaźniki LED	Dyski, stan, LAN, stan portów rozszerzenia pamięci masowej	
Obsługa RAID	RAID 0, 1, 5, 6, 10, 50, 60	
Funkcje RAID	Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD.	
Szyfrowanie	256-bitowe szyfrowanie AES folderów oraz szyfrowanie dysków zewnętrznych.	
System Operacyjny	Apple Mac OS 10.10 lub nowszy Linux and UNIX Microsoft Windows 7, 8, 10 i 11 Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016 I 2019	



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Stacja monitoringu	Tak, w standardzie 8 darmowych licencji na podłączenie kamer.	
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, FC, Telnet, SSH, SNMP	
Usługi	Stacja monitoringu Windows ACL Integracja w Windows ADS Serwer WWW Serwer plików Manager plików przez WWW Funkcja Virtual Disk umożliwiaiąca zwiększenie pojemności serwera przy pomocy protokołu iSCSI Replikacja w czasie rzeczywistym Serwer RADIUS Klient LDAP Serwer Syslog Container Station	
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.	
Język GUI	Polski	
Gwarancja i serwis	36 miesięcy gwarancji producenta na macierz i dyski twarde	
Waga	Nie więcej niż 8 kg (netto)	

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+	
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation	
Liczba kont użytkowników	4096	
Liczba grup	512	
Liczba udziałów	512	
Max ilość połączeń (CIFS)	1500	
Zasilanie	2x 300W, 100–240 V	
Wentylatory	2 x 80mm, 12VDC	
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.	
Lista funkcji które muszą być realizowane przez oprogramowanie do backupu:		
<ol style="list-style-type: none"> 1) Możliwość backupu stacji roboczych, serwerów, maszyn wirtualnych. 2) Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich 3) Program serwerowy kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10, Windows 11; Microsoft Windows Server 2000, 		



- 2003, 2008, 2012, 2016, 2019 Linux, BSD, Mac OS X
- 4) Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10, Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology
 - 5) Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików)
 - 6) Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)
 - 7) Automatyczny backup przy wyłączaniu komputera (tylko Windows)
 - 8) Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych * i ?
 - 9) Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows)
 - 10) Backup baz danych i plików poczty w trybie online i offline
 - 11) Kopie rotacyjne (wersjonowanie)
 - 12) Zapis archiwów w otwartym formacie (ZIP 64-bit)
 - 13) Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi
 - 14) Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore)
 - 15) Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej
 - 16) Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych
 - 17) Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO



- 18) Możliwość określenia liczby archiwów przechowywanych w miejscu replikacji (mniej lub więcej niż miejscu źródłowym)
- 19) Kompresja po stronie stacji roboczej
- 20) Replikacja archiwów (automatyczna lub według harmonogramu) na dodatkowy dysk twardy, NAS, serwer FTP,
- 21) Centralne sterowanie całym Systemem z jednego miejsca
- 22) Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników
- 23) Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN
- 24) Wysyłanie Alertów administracyjnych na e-mail
- 25) Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych
- 26) Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki
- 27) Automatyczna aktualizacja oprogramowania na komputerach zdalnych
- 28) Bezterminowa licencja - licencja nie może być ograniczona czasowo
- 29) Interfejs, instrukcja i pomoc techniczna w języku polskim
- 30) Rozmiar instalacji klienta < 1MB

Usługa wdrożenia:

Usługa wdrożenia powinna zostać zrealizowana

- 1) Wysyłka przygotowanej do wdrożenia macierzy NAS (przeprowadzona integracja z oprogramowaniem do backupu),



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

<p>zdalnie, a w jej zakresie powinny zawierać się przynajmniej:</p>	<ol style="list-style-type: none"> 2) Konfiguracja serwera backupu, 3) Przygotowanie paczki instalacyjnej aplikacji klienta backupu, 4) Omówienie i konfiguracja zadań backupu dla najważniejszych stacji klienckich, serwera oraz 4 hostów 5) Instruktażowe szkolenie administratora z wdrożonego systemu obejmujące przynajmniej omówienie konfiguracji i funkcji konsoli administracyjnej, procesu odzyskiwania danych oraz najlepszych praktyk dla rozwiązań backupowych. 	
--	---	--

UWAGA:

Wypełnioną i podpisaną tabelę należy złożyć wraz z ofertą.

***Prawą stroną tabeli należy wypełnić stosując słowa „spełnia” lub „nie spełnia”, zaś w przypadku żądania wykazania wpisu określonych parametrów, należy wpisać oferowane konkretne, rzeczowe wartości. W przypadku, gdy Wykonawca, w którejkolwiek z pozycji wpisze słowa „nie spełnia” lub zaoferuje niższe wartości, oferta zostanie odrzucona, gdyż jej treść nie odpowiada treści SWZ**

(Oświadczenie musi być opatrzone przez osobę lub osoby uprawnione do reprezentowania Wykonawcy kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym)



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Załącznik Nr 4f – do SWZ
Opis przedmiotu zamówienia – część nr 6

Nazwa zadania:

Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”

Nazwa Wykonawcy	Adres Wykonawcy

**Część nr 6 – Zakup oprogramowania do monitorowania urządzeń sieciowych
Specyfikacja techniczna/formularz do wypełnienia przez Wykonawcę**

Nazwa komponentu	Wymagane parametry minimalne	Potwierdzenie spełnienia wymagań (Należy wpisać SPEŁNIA oraz podać istotne parametry faktyczne)*
Typ	Oprogramowanie do monitorowania urządzeń sieciowych	Producent: Nazwa oprogramowania:
Budowa oprogramowania	modułowa, składająca się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Moduły mają umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomoc w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem.	

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00



<p>Zakres monitorowania infrastruktury</p>	<p>serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle przynajmniej w zakresie:</p> <ol style="list-style-type: none">1) Serwisów TCP/IP, http, HTTPS, POP3, SMTP, IMAP, MAPI, FTP i innych wraz z możliwością definiowania własnych serwisów. System musi monitorować m.in. czas ich odpowiedzi i procent utraconych pakietów.2) Serwerów pocztowych:<ol style="list-style-type: none">a) system musi monitorować zarówno serwis odbierający, jak i wysyłający pocztę,b) program musi mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdują się poza zakresem),c) program musi mieć możliwość wykonywania operacji testowych,d) program musi mieć możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa.3) Monitorowania serwerów WWW i adresów URL.4) Obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.5) Obsługi urządzeń SNMP wspierających SNMP v1/2/3 (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.).6) Obsługi komunikatów syslog i pułapek SNMP.	
---	--	--



	<p>7) Monitoringu routerów i przełączników wg:</p> <ul style="list-style-type: none"> a) zmian stanu interfejsów sieciowych, b) ruchu sieciowego, c) podłączonych stacji roboczych, d) ruchu generowanego przez podłączone stacje robocze. <p>8) Serwisów Windows: monitor serwisów Windows musi alarmować gdy serwis przestanie działać oraz pozwalać na jego uruchomienie / zatrzymanie / zrestartowanie.</p> <p>9) Wydajności systemów Windows:</p> <ul style="list-style-type: none"> a) obciążenie CPU, b) pamięci, c) zajętość dysków, d) transfer sieciowy. 	
<p>Automatyczne definiowanie map urządzeń</p>	<p>Zgodnie ze:</p> <ul style="list-style-type: none"> 1) zdefiniowaną przez administratora systemu strukturą organizacyjną 2) zdefiniowanymi przez administratora filtrem; minimalne kryteria, które musi umożliwiać filtr: <ul style="list-style-type: none"> a) agent: stan, wersja, zainstalowany b) alarmy: aktywne c) aplikacje: zainstalowany program (zainstalowany lub nie), wersja aplikacji (zainstalowana lub nie) d) usługi: monitorowane usługi, czas odpowiedzi e) SNMP: włączone, lokalizacja, mapowanie portów 	



	f) Właściwości urządzenia: rodzaj, nazwa, opis, adres MAC, adres IP.	
Moduł inwentaryzacji sprzętu sieciowego	<p>Automatyczne gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych. Moduł powinien:</p> <ol style="list-style-type: none"> 1) Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp. 2) Informować o m.in.: zestawieniu posiadanych konfiguracji sprzętowych, wolnym miejscu na dyskach, średnim wykorzystaniu pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 3) Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. 4) Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. 5) Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiegokolwiek zmiany konfiguracji sprzętowej komputera. 6) Umożliwiać odczytanie numeru seryjnego (klucze licencyjne) <p>Moduł inwentaryzacji sprzętu musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie:</p>	



	<p>a) przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,</p> <p>b) definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania musi istnieć możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (musi być możliwość podania daty, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX), skan dowolnego dokumentu, czy też własny komentarz; dodatkowo musi być możliwość importu danych z zewnętrznego źródła (.CSV),</p> <p>c) generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania,</p> <p>d) archiwizacji i porównywania audytów środków trwałych,</p> <p>e) tworzenia kodów kreskowych w Środkach Trwałych,</p> <p>f) drukowania kodów kreskowych oraz QR Code (mozaikowe) dla środków trwałych, które posiadają</p>	
--	---	--



	<p>numer inwentarzowy, g) inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej. Dostępne powinny być Agenty inwentaryzacji na systemy Android, OS X oraz Linux Inwentaryzacja oprogramowania musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:</p> <ul style="list-style-type: none"> a) Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. b) Zarządzanie posiadanymi licencjami. c) Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili musi istnieć możliwość wykonania aktualnych raportów audytowych. d) Zarządzanie posiadanymi licencjami: raport zgodności licencji. e) Możliwość przypisania do programów numerów seryjnych, wartości itp. <p>Okna audytowe muszą posiadać możliwość filtrowania elementów z dokładnością do jednostki.</p>	
<p>Moduł kontroli użytkowników</p>	<p>Oprogramowanie musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez analizę:</p>	



	<ol style="list-style-type: none">1) Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),2) Monitorowanie procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika),3) Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona),4) Informacji o edytowanych przez użytkownika dokumentach,5) Historii pracy (cykliczne zrzuty ekranowe),6) Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),7) Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),8) Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,9) Nagłówków przesyłanej poczty e-mail.	
--	---	--



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

	<p>Oprogramowanie ponadto musi mieć funkcjonalność blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla danej stacji roboczej z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl).</p> <p>Oprogramowanie musi mieć możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.</p> <p>Oprogramowanie musi posiadać mechanizm blokowania uruchamiania aplikacji zdefiniowanej przez administratora.</p>	
Moduł pomocy zdalnej	<p>Oprogramowanie musi umożliwiać realizację zdalnej pomocy użytkownikom. W ramach kontroli stacji użytkownika musi być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator muszą widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu musi mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W module pomocy musi znajdować się baza zgłoszeń umożliwiającą użytkownikom zgłaszanie problemów technicznych, które z kolei muszą być przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym</p>	

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00



	<p>im problemie. System musi umożliwiać użytkownikom monitorowanie procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które będą wpisywane i widoczne dla obu stron. Moduł ten musi również zawierać komunikator (czat), który musi umożliwiać przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami. Moduł pomocy musi zawierać bazę wiedzy pomagającą użytkownikom na samodzielne rozwiązywanie najbardziej typowych problemów. Moduł pomocy zdalnej musi ponadto umożliwiać:</p> <ol style="list-style-type: none">1) pobieranie listy użytkowników z Active Directory,2) przypisywanie pracowników helpdesk do kategorii zgłoszeń,3) procesowanie zgłoszeń użytkowników z wiadomości e-mail,4) dołączanie załączników do zgłoszeń,5) zrzuty ekranowe (podgląd pulpitu),6) dystrybucję oprogramowania przez Agenty,7) dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),8) zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecenia operacji następuje kolejkowanie zadania dystrybucji pliku,	
--	--	--



	<p>9) możliwość skonfigurowania automatyzacji procesowania zgłoszeń, 10) planowanie nieobecności pracowników helpdesk, 11) generowanie raportów obsługi helpdesk.</p>	
<p>Moduł ochrony danych</p>	<p>Oprogramowanie musi posiadać możliwość ochrony danych przed wyciekiem poprzez blokowanie:</p> <ol style="list-style-type: none"> 1) urządzeń i nośników danych. System musi mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. 2) urządzeń i interfejsów fizycznych: USB, FireWire, gniazd kart pamięci, dysków SATA, dysków przenośnych, napędów CD/DVD, stacji dyskietek. 3) interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. <p>Blokownie musi dotyczyć tylko urządzeń służących do przenoszenia danych - inne urządzenia korzystające z tych interfejsów (drukarka, klawiatura, mysz itp.) muszą działać prawidłowo.</p> <p>Oprogramowanie musi zapewniać zarządzanie prawami dostępu do urządzeń:</p> <ol style="list-style-type: none"> 1) Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. 2) Autoryzowanie urządzeń firmowych (np. szyfrowanych): 	



	<p>pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.</p> <p>3) Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników lub stacji roboczych.</p> <p>4) Centralną konfigurację poprzez ustawienie reguł (polityk) dla całej sieci lub wybranych stacji roboczych.</p>	
<p>Pozostałe parametry oprogramowania</p>	<p>Oprogramowanie musi zapewniać realizację audytu operacji na urządzeniach przenośnych:</p> <p>1) Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.</p> <p>2) Podłączenie/odłączenie urządzenia przenośnego.</p> <p>Oprogramowanie musi mieć możliwość integracji z usługą katalogową Active Directory w zakresie zarządzania prawami dostępu przypisanymi do użytkowników oraz grup domenowych.</p> <p>Agent na stacji roboczej musi być zabezpieczony przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora.</p> <p>Dostarczona licencja na oprogramowanie musi umożliwiać instalację dowolnej liczby serwerów zarządzania oraz konsoli zarządzających. Zamawiający musi mieć możliwość dowolnego przydziału licencji na każdy serwer zarządzania w ramach udzielonej licencji zbiorczej.</p> <p>Oprogramowanie musi być dostępny minimum w językach:</p>	



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

	polskim, angielskim, niemieckim.	
Okres licencji	Wieczysta licencja na oprogramowanie na 50 stanowisk z roczną aktualizacją do najnowszej wersji programu oraz rocznym dostępem do pomocy technicznej. Dostarczone oprogramowanie musi posiadać usługę wsparcia serwisowego realizowaną przez producenta oprogramowania przez okres nie krótszy niż 36 miesięcy od dnia dostarczenia licencji.	

UWAGA:

Wypełnioną i podpisaną tabelę należy złożyć wraz z ofertą.

***Prawą stroną tabeli należy wypełnić stosując słowa „spełnia” lub „nie spełnia”, zaś w przypadku żądania wykazania wpisu określonych parametrów, należy wpisać oferowane konkretne, rzeczowe wartości. W przypadku, gdy Wykonawca, w którejkolwiek z pozycji wpisze słowa „nie spełnia” lub zaoferuje niższe wartości, oferta zostanie odrzucona, gdyż jej treść nie odpowiada treści SWZ**

(Oświadczenie musi być opatrzone przez osobę lub osoby uprawnione do reprezentowania Wykonawcy kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym)



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

Załącznik Nr 4g – do SWZ
Opis przedmiotu zamówienia – część nr 7

Nazwa zadania:

Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”

Nazwa Wykonawcy	Adres Wykonawcy

**Część nr 7 – Zakup oprogramowania i urządzenia do ochrony brzegu sieci
Specyfikacja techniczna/formularz do wypełnienia przez Wykonawcę**

Nazwa komponentu	Wymagane parametry minimalne	Potwierdzenie spełnienia wymagań (Należy wpisać SPEŁNIA oraz podać istotne parametry faktyczne)*
Typ	Oprogramowanie i urządzenie do ochrony brzegu sieci	Producent: Typ/Model:
Wymagania ogólne	1) Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji	

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00



	<p>programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>2) System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>3) W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.</p> <p>4) System musi wspierać IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none">a) Firewall.b) Ochrony w warstwie aplikacji.c) Protokołów routingu dynamicznego.	
--	--	--



<p>Redundancja, monitoring i wykrywanie awarii</p>	<p>5) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.</p> <p>6) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.</p> <p>7) Monitoring stanu realizowanych połączeń VPN.</p> <p>8) System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.</p> <p>9) ochrona przed spamem</p>	
<p>Interfejsy, Dysk, Zasilanie</p>	<p>1) System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45 w tym:</p> <ul style="list-style-type: none"> a) min. 7 portów LANj b) min. 2 porty WAN c) min. 1 port DZM <p>2) System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</p> <p>3) W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.</p>	



	4) System musi być wyposażony w zasilanie AC.	
Parametry wydajnościowe	<ol style="list-style-type: none"> 1) W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2) Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 600 Mbps. 4) Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. 5) Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. 6) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. 7) Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps. 	
Funkcje Systemu Bezpieczeństwa	<p>W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ol style="list-style-type: none"> 1) Kontrola dostępu - zaporą ogniową klasy Stateful 	



	<p>Inspection.</p> <ol style="list-style-type: none">2) Kontrola Aplikacji.3) Poufność transmisji danych - połączenia szyfrowane IPsec VPN oraz SSL VPN.4) Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.5) Ochrona przed atakami - Intrusion Prevention System.6) Kontrola stron WWW.7) Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.8) Zarządzanie pasmem (QoS, Traffic shaping).9) Mechanizmy ochrony przed wyciekami poufnej informacji (DLP).10) Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.11) Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.12) Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z	
--	--	--



	możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system	
Polityki, Firewall	<ol style="list-style-type: none"> 1) Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2) System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: <ol style="list-style-type: none"> a) translację jeden do jeden oraz jeden do wielu. b) dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3) W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4) Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 5) Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. <ol style="list-style-type: none"> a) Amazon Web Services (AWS). b) Microsoft Azure c) Google Cloud Platform (GCP). 	



	<p>d) OpenStack. e) VMware NSX.</p>	
<p>Połączenia VPN</p>	<p>1) System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:</p> <ul style="list-style-type: none"> a) wsparcie dla IKE v1 oraz v2. b) obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). c) obsługa protokołu Diffie-Hellman grup 19 i 20. d) wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. e) tworzenie połączeń typu Site-to-Site oraz Client-to-Site. f) monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. g) możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. h) obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. i) mechanizm „Split tunneling” dla połączeń Client-to-Site. <p>2) System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:</p> <ul style="list-style-type: none"> a) pracę w trybie Portal - gdzie dostęp do chronionych 	



	<p>zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.</p> <p>b) pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.</p> <p>c) producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwi realizację połączeń IPsec VPN lub SSL VPN.</p>	
Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie powinno zapewniać obsługę:</p> <ol style="list-style-type: none"> 1) Routingu statycznego. 2) Policy Based Routingu. 3) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 	
Funkcje SD-WAN	<ol style="list-style-type: none"> 1) System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2) Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. 	
Zarządzanie pasmem	<ol style="list-style-type: none"> 1) System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2) Musi istnieć możliwość określania pasma dla 	



	poszczególnych aplikacji. 3) System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.	
Ochrona przed malware	<ol style="list-style-type: none">1) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).2) System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.3) System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).4) System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.5) System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.6) Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.	



Ochrona przed atakami	<ol style="list-style-type: none">7) Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.8) System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.9) Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.10) Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.11) System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.12) Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.13) Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	
------------------------------	--	--



<p>Kontrola aplikacji</p>	<p>14) Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>15) Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>16) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</p> <p>17) Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>18) Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.</p>	
<p>Kontrola WWW</p>	<p>1) Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</p> <p>2) W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</p> <p>3) Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.</p> <p>4) Administrator musi mieć możliwość nadpisywania kategorii</p>	



	<p>oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>5) Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.</p> <p>6) Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.</p> <p>7) W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.</p>	
<p>Uwierzytelnianie użytkowników w ramach sesji</p>	<p>1) System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:</p> <p>a) haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</p> <p>b) haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</p> <p>c) haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</p> <p>2) Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.</p> <p>3) Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych</p>	



	<p>mechanizmów: RADIUS lub API.</p> <p>4) Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</p>	
Zarządzanie	<p>1) Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.</p> <p>2) Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>3) Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.</p> <p>4) System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.</p> <p>5) System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>6) Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie</p>	



	<p>procesowania sesji oraz stanu sesji firewall.</p> <p>7) Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p>	
Logowanie	<p>1) Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.</p> <p>2) W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p> <p>3) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.</p> <p>4) Musi istnieć możliwość logowania do serwera SYSLOG.</p>	
Certyfikaty	<p>Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall.</p>	



<p>Serwisy i licencje</p>	<p>W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.</p>	
<p>Gwarancja i wsparcie</p>	<p>Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.</p>	
<p>Rozszerzone wsparcie serwisowe AHB/SOS</p>	<p>System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy. Oferent winien przedłożyć dokumenty:</p> <ol style="list-style-type: none"> 1) Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczące o gotowości świadczenia na rzecz Zamawiającego 	



	<p>wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).</p> <p>2) Certyfikat ISO 9001 podmiotu serwisującego.</p>	
Opisy do wymagań ogólnych	<p>1) W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.</p> <p>2) Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.</p>	



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

UWAGA:

Wypełnioną i podpisaną tabelę należy złożyć wraz z ofertą.

***Prawą stroną tabeli należy wypełnić stosując słowa „spełnia” lub „nie spełnia”, zaś w przypadku żądania wykazania wpisu określonych parametrów, należy wpisać oferowane konkretne, rzeczowe wartości. W przypadku, gdy Wykonawca, w którejkolwiek z pozycji wpisze słowa „nie spełnia” lub zaoferuje niższe wartości, oferta zostanie odrzucona, gdyż jej treść nie odpowiada treści SWZ**

(Oświadczenie musi być opatrzone przez osobę lub osoby uprawnione do reprezentowania Wykonawcy kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym)

UMOWA nr 272/.../2022

W dniu 2022 r. w Bierutowie, między **Miastem i Gminą Bierutów** z siedzibą w Bierutowie ul. Moniuszki 12, 56 – 420 Bierutów zwaną dalej "Zamawiającym" reprezentowanym przez:

- Burmistrza Bierutowa – Piotra Sawickiego
przy kontrasygnacie Skarbnika Miasta i Gminy Bierutów – Marii Grelak

a

firmą z siedzibą w
zarejestrowaną w Centralnej Ewidencji i Informacji Działalności Gospodarczej, NIP
lub w Krajowym Rejestrze Sądowym nr zwaną w treści umowy „Wykonawcą”, reprezentowaną przez
została zawarta umowa o następującej treści:

§ 1

Przedmiot umowy

1. Na podstawie postępowania przeprowadzonego w trybie podstawowym na podstawie art. 275 pkt 2 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2021 r., poz. 1129 ze zm.), Zamawiający powierza, a Wykonawca przyjmuje do wykonania na warunkach określonych w niniejszej umowie zadanie pn. **Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”**, zgodnie z:
 - 1) zakresem rzeczowym robót określonym w SWZ,
 - 2) ofertą Wykonawcy,będącymi integralnymi załącznikami niniejszej umowy.
2. Przedmiotem zamówienia jest **zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”**, z podziałem na następujące części:
W ramach działania cyfryzacji biur, jednostek publicznych, jednostek podległych i nadzorowanych:
Część nr 1* – Zakup serwerów;
Część nr 2* – Modernizacja wewnętrznej sieci LAN;
Część nr 3* – Zakup urządzenia wielofunkcyjnego z możliwością skanowania do sieci;
Część nr 4* – Zakup oprogramowania biurowego;

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

**Część nr 5* – Zakup systemu do tworzenia kopii bezpieczeństwa;
W ramach działania zapewnienie cyberbezpieczeństwa samorządowych systemów informatycznych:**

Część nr 6* – Zakup oprogramowania do monitorowania urządzeń sieciowych;

Część nr 7* – Zakup oprogramowania i urządzenia do ochrony brzegu sieci.

3. Na realizację przedmiotowego zamówienia Zamawiający otrzymał grant na podstawie umowy o powierzenie grantu nr 2944/1/2021 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, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00.
4. Przedmiot zamówienia obejmuje dostawę sprzętu i oprogramowania do siedziby Urzędu Miejskiego w Bierutowie:

W ramach działania cyfryzacji biur, jednostek publicznych, jednostek podległych i nadzorowanych:

Część nr 1 – zakup serwerów: serwery szt. 2 dla Urzędu Miejskiego w Bierutowie – zakup 2 serwerów w celu przystosowania do wymagań systemu umożliwiającego realizację zdalnej obsługi mieszkańców*, dla urzędu,

Część nr 2 – modernizacja wewnętrznej sieci LAN: modernizacja szkieletu sieci LAN w celu dostosowania do obowiązujących standardów, podniesienia poziomu bezpieczeństwa usług oraz przystosowanie do świadczenia zdalnych usług dla mieszkańców*, w urzędzie,

Część nr 3 – zakup urządzenia wielofunkcyjnego z możliwością skanowania do sieci: sieciowe urządzenie wielofunkcyjne szt. 1 – urządzenie niezbędne do digitalizacji dokumentów w celu usprawnienia pracy zdalnej*, dla urzędu,

Część nr 4 – zakup oprogramowania biurowego: oprogramowanie Microsoft 365 (zakup licencji na 18 miesięcy) – 90 licencji dla urzędu i jednostek podległych*,

Część nr 5 – zakup systemu do tworzenia kopii bezpieczeństwa: system do backup szt. 1 – zapewnienie ciągłości działania systemów informatycznych dla urzędu*,

W ramach działania zapewnienie cyberbezpieczeństwa samorządowych systemów informatycznych:

Część nr 6 – zakup oprogramowania do monitorowania urządzeń

sieciowych: specjalistyczne oprogramowanie do ochrony danych i inwentaryzacji zasobów sieciowych*, dla urzędu,

Część nr 7 – zakup oprogramowania i urządzenia do ochrony brzegu sieci:

specjalistyczne oprogramowanie i urządzenie do ochrony brzegu sieci dla urzędu*.

5. Szczegółowy opis przedmiotu zamówienia zawarty jest w Specyfikacjach technicznych stanowiących załączniki nr 4a-4g do SWZ dla danej części. Specyfikacja techniczna zawiera minimalne wymagania, które musi spełniać oferowany przedmiot zamówienia.
6. Wykonawca zobowiązuje się do prawidłowego wykonania przedmiotu zamówienia, zgodnie z wymaganiami określonymi w Specyfikacji Warunków Zamówienia i postanowieniami projektu umowy oraz zasadami wiedzy technicznej, zasadami należytej staranności oraz obowiązującymi normami i przepisami.
7. Adres dostawy przedmiotu zamówienia: ul. Moniuszki 12, 56-420 Bierutów.
8. O terminie dostawy Wykonawca zobowiązany jest zawiadomić Zamawiającego co najmniej z 2-dniowym wyprzedzeniem. Dostawa przedmiotu umowy nastąpi w godzinach 8:00-14:00.
9. Wykonawca zobowiązuje się dostarczyć przedmiot Zamówienia na własny koszt i ryzyko do miejsca wskazanego przez Zamawiającego.
10. Wykonawca musi zagwarantować możliwość ewentualnych napraw dostarczonego sprzętu. Dane teleadresowe punktu serwisowego Wykonawca wskaże w protokole odbioru dostarczonego sprzętu.
11. Wykonawca zobowiązuje się do dostarczenia sprzętu fabrycznie nowego, nieużywanego, wolnego od wad fizycznych i prawnych oraz wydania dokumentacji dotyczącej dostarczonego przedmiotu zamówienia np. certyfikatów, atestów, deklaracji zgodności, instrukcji obsługi itp.
12. Odbiór zadania nastąpi w formie protokołu, po uprzednim stwierdzeniu jego zgodności z warunkami zamówienia.

§ 2

Terminy realizacji przedmiotu umowy

Termin wykonania przedmiotu zamówienia:

- 1) **Część nr 1*:** dodni od dnia zawarcia umowy;
- 2) **Część nr 2*:** dodni od dnia zawarcia umowy;

- 3) **Część nr 3*:** dodni od dnia zawarcia umowy;
- 4) **Część nr 4*:** dodni od dnia zawarcia umowy;
- 5) **Część nr 5*:** dodni od dnia zawarcia umowy;
- 6) **Część nr 6*:** dodni od dnia zawarcia umowy;
- 7) **Część nr 7*:** dodni od dnia zawarcia umowy.

§ 3

Wynagrodzenie, zasady rozliczenia i płatności

1. Strony ustalają, iż obowiązującą formą wynagrodzenia za wykonanie przedmiotu umowy jest wynagrodzenie ryczałtowe zgodnie z przedstawionym formularzem ofertowym.
2. Za wykonanie przedmiotu umowy Zamawiający zapłaci Wykonawcy wynagrodzenie nettoplus podatek VAT 23% w kwociezł, łącznie brutto w wysokości: PLN (słownie: zł), w tym:
 - 1) **Część nr 1** – wynagrodzenie nettoplus podatek VAT 23% w kwociezł, łącznie brutto w wysokości: PLN (słownie: zł)*,
 - 2) **Część nr 2** – wynagrodzenie nettoplus podatek VAT 23% w kwociezł, łącznie brutto w wysokości: PLN (słownie: zł)*
 - 3) **Część nr 3** – wynagrodzenie nettoplus podatek VAT 23% w kwociezł, łącznie brutto w wysokości: PLN (słownie: zł)*
 - 4) **Część nr 4** – wynagrodzenie nettoplus podatek VAT 23% w kwociezł, łącznie brutto w wysokości: PLN (słownie: zł)*
 - 5) **Część nr 5** – wynagrodzenie nettoplus podatek VAT 23% w kwociezł, łącznie brutto w wysokości: PLN (słownie: zł)*
 - 6) **Część nr 6** – wynagrodzenie nettoplus podatek VAT 23% w kwociezł, łącznie brutto w wysokości: PLN (słownie: zł)*
 - 7) **Część nr 7** – wynagrodzenie nettoplus podatek VAT 23% w kwociezł, łącznie brutto w wysokości: PLN (słownie: zł)*

3. Rozliczenie za wykonanie przedmiotu zamówienia odbędzie się na podstawie faktury VAT wystawionej przez Wykonawcę.
4. Podstawą do wystawienia faktury VAT jest protokół odbioru przedmiotu zamówienia, stanowiący załącznik do niniejszej umowy, nie zawierający uwag, podpisany przez przedstawicieli Zamawiającego i Wykonawcy.
5. Faktura zostanie wystawiona przez Wykonawcę na:
Nabywca: Miasto i Gmina Bierutów, ul. Moniuszki 12, 56 – 420 Bierutów, NIP 911-17-77-417
Odbiorca: Urząd Miejski w Bierutowie, ul. Moniuszki 12, 56 – 420 Bierutów.
i doręczona na adres: Urząd Miejski w Bierutowie, ul. Moniuszki 12, 56-420 Bierutów.
6. Płatność za fakturę VAT, o której mowa w ust. 3 będzie dokonywana przelewem na konto wskazane na fakturze przez Wykonawcę w terminie do 21 dni licząc od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury i po spełnieniu warunków wyżej opisanych.
7. Wynagrodzenie uwzględnia wszystkie koszty, jakie poniesie Wykonawca z tytułu należytej i zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia, bez prawa odrębnego dochodzenia ich zwrotu.

§ 4

Obowiązki Stron

1. Wykonawca zobowiązuje się do prawidłowego wykonania przedmiotu Umowy, zgodnie z postanowieniami niniejszej umowy oraz Specyfikacją Warunków Zamówienia, zasadami wiedzy technicznej, zasadami należytej staranności oraz obowiązującymi normami i przepisami.
2. Przedmiot zamówienia, o którym mowa w § 1 należy dostarczyć na adres: ul. Moniuszki 12, 56-420 Bierutów.
3. O terminie dostawy Wykonawca zobowiązany jest zawiadomić Zamawiającego co najmniej z 2-dniowym wyprzedzeniem. Dostawa przedmiotu umowy nastąpi w godzinach 8:00-14:00.
4. Wykonawca zobowiązuje się dostarczyć przedmiot Zamówienia na własny koszt i ryzyko do miejsca wskazanego przez Zamawiającego.
5. Wykonawca zobowiązuje się do dostarczenia przedmiotu umowy, nieużywanego, wolnego od wad fizycznych i prawnych oraz wydania dokumentacji dotyczącej dostarczonego przedmiotu zamówienia np. certyfikatów, atestów, deklaracji zgodności, instrukcji obsługi itp.

6. Odbiór przedmiotu umowy nastąpi w formie protokołu, po uprzednim stwierdzeniu jego zgodności z warunkami zamówienia.
7. Przez okres gwarancji serwis urządzeń będzie realizowany przez producenta lub autoryzowanego partnera serwisowego producenta.

§ 5

Podwykonawcy

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy, z zastrzeżeniem ustępów poniższych.
2. Zamawiający żąda, ponieważ dostawy mają być wykonane w miejscu podlegającym bezpośredniemu nadzorowi zamawiającego, aby przed przystąpieniem do wykonania zamówienia Wykonawca, o ile są już znane, podał nazwy albo imiona i nazwiska oraz dane kontaktowe podwykonawców i osób do kontaktu z nimi, zaangażowanych w takie dostawy. Wykonawca zawiadamia zamawiającego o wszelkich zmianach danych, o których mowa w zdaniu pierwszym, w trakcie realizacji zamówienia, a także przekazuje informacje na temat nowych podwykonawców, którym w późniejszym okresie zamierza powierzyć realizację dostaw.
3. Wykonawca będzie w pełni odpowiedzialny za działania lub uchybienia każdego podwykonawcy, dostawcy, usługodawcy i ich przedstawicieli lub pracowników, tak jakby były to działania lub uchybienia Wykonawcy. Wykonawca jest zobowiązany do terminowego regulowania wszelkich zobowiązań wobec podwykonawców, dostawców i usługodawców, z którymi współpracuje w związku z realizacją umowy. Nieterminowe regulowanie wymagalnych zobowiązań wobec wyżej wskazanych podmiotów stanowi nienależyte wykonywanie umowy i uprawnia Zamawiającego do dokonania wypłaty kwot z wynagrodzenia Wykonawcy, w celu dokonania zapłaty należności na rzecz Podwykonawców, Dostawców lub Usługodawców.
4. Wykonawca może w trakcie realizacji niniejszej umowy zmienić bądź zrezygnować z podwykonawcy, na którego zasoby powoływał się w celu wykazania spełniania warunków, o których mowa w rozdziale XVI SWZ. Zobowiązany jest w takim przypadku wykazać Zamawiającemu, iż nowy podwykonawca lub Wykonawca samodzielnie spełnia te warunki w stopniu nie mniejszym niż było to wymagane na etapie postępowania o zamówienie publiczne.

5. Jeżeli powierzenie podwykonawcy wykonania części zamówienia dostaw następuje w trakcie jego realizacji, wykonawca na żądanie zamawiającego przedstawia oświadczenie, o którym mowa w art. 125 ust. 1 ustawy pzp.
6. Płatności.
 - 1) Warunkiem zapłaty przez Zamawiającego należnego wynagrodzenia Wykonawcy jest przedstawienie dowodów zapłaty wymaganego wynagrodzenia Podwykonawcy, biorącym udział w realizacji zamówienia.
 - 2) W przypadku uchylania się przez Wykonawcę, podwykonawcę zamówienia od obowiązku zapłaty, Zamawiający dokona bezpośredniej zapłaty wymaganego wynagrodzenia przysługującego podwykonawcy, który zawarł przedłożoną Zamawiającemu umowę o podwykonawstwo, której przedmiotem są dostawy i usługi,
 - 3) Wynagrodzenie, o którym mowa w pkt 2 dotyczy wyłącznie należności powstałych po przedłożeniu Zamawiającemu poświadczonej za zgodność z oryginałem kopii umowy o podwykonawstwo, której przedmiotem są dostawy lub usługi,
 - 4) Bezpośrednia zapłata obejmuje wyłącznie należne wynagrodzenie, bez odsetek. należnych Podwykonawcy,
 - 5) Przed dokonaniem bezpośredniej zapłaty Zamawiający wezwie Wykonawcę, do zgłoszenia pisemnych uwag dotyczących zasadności bezpośredniej zapłaty wynagrodzenia podwykonawcy w terminie 7 dni od dnia doręczenia tej informacji,
 - 6) W przypadku zgłoszenia we wskazanym terminie uwag, o których mowa w pkt 5, Zamawiający może:
 - nie dokonać bezpośredniej zapłaty wynagrodzenia Podwykonawcy, jeżeli wykonawca wykaże niezasadność takiej zapłaty, albo
 - złożyć do depozytu sądowego kwotę potrzebną na pokrycie wynagrodzenia Podwykonawcy w przypadku istnienia zasadniczej wątpliwości Zamawiającego co do wysokości należnej zapłaty lub podmiotu, któremu płatność się należy, albo
 - dokonać bezpośredniej zapłaty wynagrodzenia Podwykonawcy, jeżeli Podwykonawca lub dalszy podwykonawca wykaże zasadność takiej zapłaty.

- 7) Zapłata przez Zamawiającego na rzecz Podwykonawcy dokonana będzie w terminie do 30 dni od dnia zgłoszenia roszczenia wraz z kompletem wymaganych dokumentów,
- 8) W przypadku dokonania bezpośredniej zapłaty Podwykonawcy, o których mowa w pkt 4, Zamawiający potrąca kwotę wypłaconego wynagrodzenia z wynagrodzenia należnego Wykonawcy.
7. Odstąpienie od umowy w przypadku naruszenia obowiązków Wykonawcy wobec podwykonawców.
Zamawiający może odstąpić od umowy z Wykonawcą, jeżeli:
 - 1) zaistnieje konieczność dwukrotnego dokonywania bezpośredniej zapłaty Podwykonawcy,
 - 2) zaistnieje konieczność dokonania dwóch bezpośrednich zapłat na sumę większą niż 5% wartości umowy określonej w § 3 ust. 2.
8. Zlecenie części prac Podwykonawcy(om) nie zmienia zobowiązań Wykonawcy wobec Zamawiającego do wykonania prac powierzonych Podwykonawcy(om).
9. Wykonawca jest zobowiązany do należytego wykonywania umowy zawartej przez siebie z Podwykonawcą.

§ 6

Nadzór nad wykonywanymi dostawami

Strony ustanawiają osoby upoważnione do kontaktów i nadzoru nad realizacją przedmiotu umowy:

- 1) Z ramienia Wykonawcy:

....., tel.

- 2) Z ramienia Zamawiającego:

Roman Członkowski – Informatyk, tel. 71-314-62-51 wew. 53

§ 7

Gwarancja i rękojmia za wady

1. Wykonawca udziela gwarancji i rękojmi, że przedmiot dostawy jest fabrycznie nowy i wolny od wad, oraz że może być użytkowany zgodnie z przeznaczeniem, wręczając Zamawiającemu, w dniu protokolarnego odbioru przedmiotu zamówienia, dokumenty gwarancyjne.
2. Okres gwarancji i rękojmi przedmiotu zamówienia liczony będzie od dnia protokolarnego odbioru przedmiotu zamówienia.

3. Wykonawca zobowiązuje się do bezpłatnego wykonania naprawy gwarancyjnej przedmiotu umowy nie później niż w ciągu 3 dni od momentu zgłoszenia usterki.
4. W przypadku naprawy komputerów przenośnych, okres gwarancji ulegnie przedłużeniu o okres wykonywania naprawy; natomiast w przypadku dokonania wymiany komputerów przenośnych okres gwarancji zostanie ustalony zgodnie z gwarancją nowego sprzętu.
5. Odpowiedzialność z tytułu gwarancji jakości obejmuje zarówno wady powstałe z przyczyn tkwiących w wyposażeniu objętym przedmiotem umowy w chwili dokonania jego odbioru przez Zamawiającego, jak i wszelkie inne wady fizyczne powstałe z przyczyn, za które Wykonawca lub inny gwarant ponosi odpowiedzialność, pod warunkiem, że wady te ujawnią się w okresie obowiązywania gwarancji.
6. Jeżeli w terminie, o którym mowa w § 7 ust. 2 ujawnią się takie wady fizyczne przedmiotu umowy, które nie kwalifikują się do ich usunięcia, bądź jeżeli przedmiot umowy był naprawiany co najmniej 2 – krotnie, Wykonawca zobowiązuje się do dostarczenia przedmiotu umowy wolnego od wad o parametrach nie gorszych lub lepszych. W przypadku ziszczenia się obowiązku wymiany przedmiotu umowy na nowy, Wykonawca zobowiązuje się do tego w terminie 3 dni roboczych od momentu powstania obowiązku wymiany.
7. W przypadku niedotrzymania terminu naprawy gwarancyjnej, bądź niedotrzymania terminu wymiany przedmiotu zamówienia na wolny od wad, Zamawiający jest uprawniony do usunięcia wad w drodze naprawy na ryzyko i koszt Wykonawcy, zachowując przy tym inne uprawnienia przysługujące mu na podstawie Umowy, a w szczególności roszczenia z tytułu rękojmi za wady fizyczne lub Zamawiający będzie naliczał karę umowną w wysokości 100,00 zł za każdy dzień zwłoki.
8. Szczegółowe warunki gwarancji określi dokument gwarancyjny. Postanowienia dokumentu gwarancyjnego sprzeczne z odpowiednimi postanowieniami zawartymi w niniejszej umowie są nieważne, w ich miejsce zastosowanie znajdują odpowiednie postanowienia niniejszej umowy. Nie dotyczy to postanowień korzystniejszych dla Zamawiającego, a zwłaszcza wydłużenia terminów określonych w § 7 ust. 2 umowy.
9. Wykonawca jest odpowiedzialny względem Zamawiającego za wszelkie wady prawne przedmiotu umowy, w tym również za ewentualne roszczenia.

§ 8

Kary umowne

1. Wykonawca zapłaci Zamawiającemu kary umowne:
 - 1) za każdy dzień zwłoki w oddaniu przedmiotu zamówienia objętego kontraktem w wysokości 0,2% wynagrodzenia ryczałtowego brutto, o którym mowa w § 3 ust. 2,
 - 2) za każdy dzień zwłoki w terminie usunięcia wad w wysokości 0,2% wynagrodzenia ryczałtowego brutto, o którym mowa w § 3 ust. 2,
 - 3) w przypadku odstąpienia przez wykonawcę od realizacji zawartej umowy w wysokości 30% wartości umowy,
 - 4) w przypadku odstąpienia od umowy przez zamawiającego z wyłącznej winy wykonawcy, wykonawca zapłaci zamawiającemu odszkodowanie w wysokości 30% ceny umownej brutto.
2. Kary umowne w zakresie obowiązków Wykonawcy związanych z zatrudnianiem Podwykonawców:

Wykonawca zapłaci Zamawiającemu następujące kary umowne:

 - 1) z tytułu braku zapłaty wynagrodzenia należnego Podwykonawcom w wysokości 5% wartości wynagrodzenia brutto należnego Podwykonawcom,
 - 2) z tytułu nieterminowej zapłaty wynagrodzenia należnego Podwykonawcom w wysokości 0,01 % wartości wynagrodzenia brutto należnego Podwykonawcom za każdy dzień przekroczenia terminu,
 - 3) z tytułu nieprzedłożenia poświadczonych za zgodność z oryginałem kopii umowy o podwykonawstwo lub jej zmiany w wysokości 0,01 % wartości umownej brutto wymienionej w § 3 ust.2,
3. Odstąpienie od umowy w przypadku naruszenia obowiązków Wykonawcy wobec podwykonawców - wykonawca zapłaci zamawiającemu odszkodowanie w wysokości 30% wynagrodzenia brutto, o którym mowa w § 3 ust. 2.

Zamawiający może odstąpić od umowy z Wykonawcą, jeżeli:

 - 1) zaistnieje konieczność dwukrotnego dokonywania bezpośredniej zapłaty Podwykonawcy,
 - 2) zaistnieje konieczność dokonania dwóch bezpośrednich zapłat na sumę większą niż 5% wartości umowy określonej w § 3 ust. 2.
4. Zlecenie części prac Podwykonawcy(om) nie zmienia zobowiązań Wykonawcy wobec Zamawiającego do wykonania prac powierzonych Podwykonawcy(om).
5. Wykonawca jest zobowiązany do należytego wykonywania umowy zawartej przez siebie z Podwykonawcą.

6. Łączna wartość należnych zamawiającemu kar umownych, o których mowa w ust. 1-3, nie może przekroczyć 50% wynagrodzenia brutto, o którym mowa w § 3 ust. 2.
7. Wykonawca upoważnia Zamawiającego do potrącenia należnych kar z przysługującego mu wynagrodzenia.
8. Strony zastrzegają możliwość dochodzenia odszkodowania przenoszącego wysokość zastrzeżonych kar umownych na zasadach ogólnych.

§ 9

Odstąpienie od umowy

1. Strony mogą rozwiązać umowę na podstawie pisemnego porozumienia.
2. W przypadku stwierdzenia wad nadających się do usunięcia Zamawiający zastrzega sobie prawo odmowy odbioru prac i wyznaczenie terminu usunięcia wad. Po upływie wyżej wymienionego terminu naliczane będą kary umowne określone w § 8.
3. W przypadku stwierdzenia wad nie nadających się do usunięcia jeżeli nie uniemożliwiają one użytkowania przedmiotu umowy zgodnie z przeznaczeniem, Zamawiający zastrzega sobie prawo do obniżenia odpowiednio wynagrodzenia.
4. W przypadku stwierdzenia wad nie nadających się do usunięcia jeżeli wady uniemożliwiają użytkowanie przedmiotu umowy zgodnie z przeznaczeniem, Zamawiający może od umowy odstąpić w terminie 30 dni licząc od dnia powzięcia informacji o wadach.
5. W przypadku zwłoki z przyczyn leżących po stronie Wykonawcy dłuższego niż 30 dni w wykonaniu Przedmiotu umowy, Zamawiający zastrzega sobie prawo odstąpienia od umowy bez konieczności wyznaczania dodatkowego terminu do wykonania umowy w terminie 30 dni licząc od 31 dnia zwłoki.
6. Zamawiającemu przysługuje prawo do złożenia oświadczenia o odstąpieniu od Umowy w terminie 30 dni od pisemnego wezwania, o którym mowa w pkt 1-3 i w pkt 7 oraz w terminie 30 dni od powzięcia wiadomości o okolicznościach, o których mowa w pkt 4-6 i 8-9:
 - 1) Wykonawca nie przystąpił do realizacji Przedmiot Umowy w terminie zgodnym z postanowieniami niniejszej Umowy, pomimo pisemnego wezwania Wykonawcy przez Zamawiającego,
 - 2) Wykonawca przerwał realizację Przedmiotu Umowy z przyczyn leżących po stronie Wykonawcy i przerwa ta trwa dłużej niż 14 dni, pomimo pisemnego wezwania,

- 3) Wykonawca realizuje Przedmiot Umowy w sposób niezgodny ze wskazaniami Zamawiającego lub Umową, pomimo pisemnego wezwania Wykonawcy przez Zamawiającego do realizacji Przedmiotu Umowy zgodnie z tym dokumentem,
 - 4) w wyniku wszczętego postępowania egzekucyjnego nastąpi zajęcie majątku Wykonawcy, w całości lub znacznej części, w takim zakresie, że nie będzie możliwa dalsza realizacja prac przez Wykonawcę,
 - 5) Wykonawca podzleca zamówienie w całości lub w części bez wiedzy Zamawiającego,
 - 6) sytuacja ekonomiczna Wykonawcy ulegnie znacznemu pogorszeniu lub Wykonawca zostanie postawiony w stan likwidacji,
 - 7) Wykonawca wykonuje swoje obowiązki w sposób niezgodny z Umową lub bez zachowania wymaganej staranności, nie dostosowuje się w wyznaczonym terminie do wezwania przesłanego mu przez Zamawiającego z żądaniem zaniechania zaniedbań lub nie spełnienia obowiązków wynikających z Umowy, co poważnie wpływa na właściwą i terminową realizację Umowy,
 - 8) nastąpi utrata zdolności do czynności prawnych,
 - 9) jeżeli wartość kar umownych, którymi Zamawiający obciążył Wykonawcę zgodnie z § 8 Umowy, przekroczy kwotę 50 % wynagrodzenia brutto Wykonawcy.
7. W razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, lub dalsze wykonywanie umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, zamawiający może odstąpić od umowy w terminie 30 dni od dnia powzięcia wiadomości o tych okolicznościach.
8. Zamawiający może odstąpić od umowy w przypadkach określonych w art. 456 ust. 1 lub ust. 2 ustawy Prawo zamówień publicznych.
9. W przypadku, o którym mowa w ust. 5 - 8 Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy do chwili jej rozwiązania stosownie do zapisów zawartych w § 3 niniejszej umowy.
10. W przypadku odstąpienia od Umowy, Wykonawcę i Zamawiającego obciążają następujące obowiązki szczegółowe:
- 1) w terminie do 7 dni od daty odstąpienia od Umowy, Wykonawca przy udziale Zamawiającego, sporządzi szczegółową inwentaryzację wykonanych prac,

- według stanu na dzień odstąpienia,
- 2) Wykonawca niezwłocznie zabezpieczy przerwane prace w zakresie obustronnie uzgodnionym, na koszt strony, z winy której nastąpiło odstąpienie od Umowy,
 - 3) w terminie do 7 dni od daty odstąpienia od Umowy, Wykonawca sporządzi wykaz tych materiałów, konstrukcji zakupionych do realizacji Umowy, które nie mogą być wykorzystane przez Wykonawcę do realizacji innych prac (jeśli dotyczy),
 - 4) Wykonawca niezwłocznie, nie później niż do 3 dni od odstąpienia od Umowy, zgłosi Zamawiającemu do odbioru prace przerwane oraz zabezpieczające, a Zamawiający dokona ich odbioru w terminie nie dłuższym niż 7 dni od dnia zgłoszenia. Najpóźniej w terminie 14 dni od daty odstąpienia od Umowy, Wykonawca usunie z terenu montażu urządzenia przez niego dostarczone. W przypadku nie wykonania tego obowiązku, dokona tego Zamawiający na ryzyko i koszt Wykonawcy. Poniesione z tego tytułu koszty zostaną potrącone z Wynagrodzenia Wykonawcy (jeśli dotyczy),
 - 5) Wykonawca przy udziale Zamawiającego w terminie do 7 dni od dnia odstąpienia, sporządzi szczegółowy protokół inwentaryzacji prac w toku, wraz z zestawieniem wartości wykonanych prac według stanu na dzień odstąpienia, protokół inwentaryzacji prac w toku, który stanowić będzie podstawę do wystawienia faktury VAT przez Wykonawcę (jeśli dotyczy).
11. W razie odstąpienia od Umowy przez jedną ze stron, Zamawiający zobowiązany jest do dokonania odbioru przerwanych i zinwentaryzowanych prac, które zostały wykonane do dnia odstąpienia od Umowy.
12. Zamawiający składając oświadczenie o odstąpieniu wskaże, czy odstępuje od Umowy w całości ze skutkiem *ex tunc* czy w części niewykonanej - *ex nunc*. W przypadku odstąpienia w części niewykonanej (*ex nunc*) z momentem złożenia oświadczenia o odstąpieniu dla części Przedmiotu Umowy, dla których sporządzono i przekazano Wykonawcy protokoły odbioru Etapów realizacji Przedmiotu Umowy rozpoczyna się bieg okresu rękojmi oraz gwarancji (na warunkach określonych w Umowie).

§ 10

Zmiana umowy

1. Na podstawie art. 455 ust. 1 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych, Zamawiający przewiduje możliwość dokonania zmian

postanowień umowy zawartej z wybranym wykonawcą w następujących przypadkach:

- 1) zmiany wynagrodzenia umownego Wykonawcy, które może ulec zmianie w następujących warunkach:
 - a) w przypadku niezawinionych przez Wykonawcę okoliczności powodujących opóźnienie w realizacji Przedmiotu Umowy Zamawiający może odstąpić od naliczania kar umownych,
 - b) w przypadku zmiany stawki VAT – jeśli zmiana stawki VAT będzie powodować zwiększenie kosztów wykonania robót po stronie Wykonawcy, Zamawiający dopuszcza możliwość zwiększenia wynagrodzenia Wykonawcy o kwotę równą różnicy w kwocie podatku VAT zapłaconego przez Wykonawcę. Jeśli zmiana stawki VAT będzie powodować zmniejszenie kosztów wykonania robót po stronie Wykonawcy, Zamawiający dopuszcza możliwość zmniejszenia wynagrodzenia o kwotę stanowiącą różnicę kwoty podatku VAT zapłaconego przez Wykonawcę,
- 2) zmiana treści umowy – jeżeli zajdzie potrzeba w sytuacji zmiany obowiązujących przepisów, jeżeli zgodnie z nimi konieczne będzie dostosowanie treści umowy do aktualnego stanu prawnego,
- 3) zmiana terminu wykonania zamówienia w sytuacjach wystąpienia:
 - a) przestoju w realizacji Przedmiotu umowy, niezawinionego przez Wykonawcę, a wynikłego ze zdarzeń losowych lub decyzji Zamawiającego,
 - b) wskutek wystąpienia okoliczności niezależnych od stron umowy związanych z koniecznością zmiany okresu realizacji umowy,
- 4) zmiana wykonawcy lub podwykonawcy:

zmiana umowy może nastąpić również w wyniku zmiany wykonawcy, podwykonawcy lub rezygnacji z udziału podwykonawcy przy realizacji przedmiotu umowy. Zamawiający dopuści zmianę pod warunkiem, że nowy wykonawca wykaże, że nie podlega wykluczeniu z postępowania na warunkach określonych przez Zamawiającego w postępowaniu o udzielenie zamówienia publicznego oraz wykaże, że spełnia warunki udziału w postępowaniu w zakresie nie mniejszym niż wskazanym przez Zamawiającego na etapie postępowania o udzielenie zamówienia przez dotychczasowego wykonawcę,
- 5) zmiany będą korzystne dla Zamawiającego i nie będą:
 - a) wprowadzane warunki, które gdyby zostały ujęte w ramach procedury

- przetargowej udzielenia zamówienia umożliwiłyby dopuszczenie innych ofert niż ta, która została pierwotnie dopuszczona;
- b) modyfikowały równowagi ekonomicznej umowy na korzyść wykonawcy w sposób, który nie był przewidziany w postanowieniach pierwotnego zamówienia;
- c) istotne w rozumieniu w art. 454 ust. 2 ustawy Prawo zamówień publicznych.
2. Warunki dokonania zmian:
- 1) Strona występująca o zmianę postanowień niniejszej umowy zobowiązana jest do udokumentowania zaistnienia okoliczności, o których mowa powyżej,
- 2) Strona występująca o zmianę postanowień niniejszej umowy zobowiązana jest do złożenia pisemnego wniosku o zmianę postanowień umowy,
- 3) Wniosek, o którym mowa w pkt 2) musi zawierać:
- a) opis propozycji zmiany,
- b) uzasadnienie zmiany,
- c) opis wpływu zmiany na warunki realizacji umowy.
3. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.

§ 11

Szczegółowe regulacje dotyczące Wykonawców wspólnie ubiegających się o udzielenie zamówienia, w tym konsorcjum

1. Dla uniknięcia wątpliwości Strony potwierdzają, że w przypadku gdy Umowę zawarli z Zamawiającym Wykonawcy wspólnie ubiegający się o udzielenie zamówienia, do wykonania wszystkich zobowiązań wynikających z Umowy zobowiązani są wszyscy Wykonawcy solidarnie (solidarność dłużników).
2. Wymagania co do sposobu zawierania przez Wykonawców wspólnie ubiegających o udzielenie Zamówienia umów o podwykonawstwo zostały określone w § 5 Umowy.
3. Zabezpieczenie wniesione przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia winno zabezpieczać roszczenia Zamawiającego związane z niewykonaniem lub nienależytym wykonaniem Umowy przez każdego z Wykonawców.
4. W przypadku, gdy Umowę zawrą z Zamawiającym Wykonawcy wspólnie ubiegający się o udzielenie zamówienia:
- 1) umowa określająca wzajemne stosunki pomiędzy wykonawcami wspólnie ubiegającymi się o udzielenie zamówienia (umowa konsorcjum) winna być

przedłożona Zamawiającemu przed podpisaniem niniejszej Umowy w formie kopii potwierdzonej za zgodność z oryginałem,

- 2) umowa określająca wzajemne stosunki pomiędzy Wykonawcami wspólnie ubiegającymi się o udzielenie zamówienia (umowa konsorcjum) winna wskazywać jednoznacznie, który z Wykonawców będzie pełnił funkcję Lidera Konsorcjum,
- 3) umowa określająca wzajemne stosunki pomiędzy Wykonawcami wspólnie ubiegającymi się o udzielenie zamówienia (umowa konsorcjum) winna wskazywać jednoznacznie, na konto którego z Wykonawców Zamawiający będzie zobowiązany do uiszczania wynagrodzenia.
W przypadku konsorcjum wskazania dokonuje Lider Konsorcjum.
- 4) każdy przedstawiciel Wykonawcy winien być umocowany przez wszystkich Wykonawców do samodzielnego działania w imieniu każdego z nich,
- 5) korespondencja związana z wykonywaniem Umowy winna być podpisana przez osobę umocowaną do reprezentowania wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia.

§ 12

Klauzula salwatoryjna

1. Jeżeli część postanowień niniejszej Umowy stanie się nieważna na skutek sprzeczności z prawem, zasadami współżycia społecznego lub innych wad, Umowa pomiędzy stronami pozostaje w mocy w części w jakiej nie dotyczy jej ustawowa sankcja nieważności.
2. W przypadku o jakim mowa w ust. 1 niniejszego paragrafu Strony zobowiązane będą zawrzeć aneks do Umowy, w którym sformułują postanowienia zastępcze, których cel gospodarczy i ekonomiczny będzie równoważny lub maksymalnie zbliżony do celu postanowień nieważnych lub nieskutecznych.

§ 13

Klauzula informacyjna o przetwarzaniu danych osobowych

1. 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:

- 1) administratorem Pani/Pana danych osobowych jest Burmistrz Bierutowa, wykonujący swoje zadania przy pomocy Urzędu Miejskiego w Bierutowie, zlokalizowanego w Bierutowie przy ul. Moniuszki 12;
- 2) w sprawach związanych z Pani/Pana danymi proszę kontaktować się z Inspektorem Ochrony Danych, kontakt pisemny za pomocą poczty tradycyjnej na adres: Urząd Miejski w Bierutowie, ul. Moniuszki 12, 56-420 Bierutów, pocztą elektroniczną na adres e-mail: iod@bierutow.pl;
- 3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu prowadzenia przedmiotowego postępowania o udzielenie zamówienia publicznego oraz zawarcia umowy, a podstawą prawną ich przetwarzania jest obowiązek prawny stosowania sformalizowanych procedur udzielania zamówień publicznych spoczywający na Zamawiającym;
- 4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy Pzp;
- 5) Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
- 6) obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje nie podania określonych danych wynikają z ustawy Pzp;
- 7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- 8) posiada Pan/Pani:
 - a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących (w przypadku, gdy skorzystanie z tego prawa wymagałoby po stronie administratora niewspółmiernie dużego wysiłku może zostać Pani/Pan zobowiązana do wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego lub konkursu albo sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia),
 - b) na podstawie art. 16 RODO prawo do sprostowania lub uzupełnienia

Pani/Pana danych osobowych, przy czym skorzystanie z prawa do sprostowania lub uzupełnienia nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników,

- c) 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, przy czym prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego, a także nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia,
 - d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- 9) nie przysługuje Pani/Panu:
- a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych,
 - b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,
 - c) 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;
- 10) przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Pana danych osobowych przez administratora. Organem właściwym dla przedmiotowej skargi jest Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.
2. Jednocześnie Zamawiający przypomina o ciążyącym na Pani/Panu obowiązku informacyjnym wynikającym z art. 14 RODO względem osób fizycznych, których dane przekazane zostaną Zamawiającemu w związku z prowadzonym postępowaniem i które Zamawiający pośrednio pozyska od wykonawcy biorącego udział w postępowaniu, chyba że ma zastosowanie co najmniej jedno z wyłączeń, których mowa w art. 14 ust. 5 RODO.

§ 14

Rozstrzygnięcie sporów

Wszelkie spory wynikłe lub powstałe na tle wykonania niniejszej umowy strony będą starały się rozstrzygnąć w drodze negocjacji, a w wypadku nie osiągnięcia porozumienia poddane zostaną rozstrzygnięciu sądu powszechnego właściwego dla siedziby Zamawiającego.

§ 15

Postanowienia końcowe

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej w postaci aneksu pod rygorem nieważności.
2. W sprawach nie uregulowanych niniejszą umową mają zastosowanie przepisy ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2021 r., poz. 1129 ze zm.) oraz przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeksu Cywilnego (Dz. U. z 2020 r., poz. 1740 ze zm.).
3. W czasie trwania niniejszej Umowy, Wykonawca będzie spełniać wymagania prawne zgodnie z Ustawą o Ochronie Danych Osobowych, a także innych przepisów prawa w celu prawidłowego wykonania niniejszej Umowy.
4. Podanie danych osobowych jest niezbędne do zawarcia i wykonywania umowy.
5. Dane osobowe wskazane w umowie (oraz w załącznikach do niej) będą przetwarzane w celu jej zawarcia i wykonania.
6. Integralną częścią niniejszej umowy są:
 - 1) Specyfikacja Warunków Zamówienia,
 - 2) Oferta wykonawcy.
7. Umowę i załączniki sporządzono w 4 egzemplarzach, z przeznaczeniem: 3 egzemplarze dla Zamawiającego i 1 dla Wykonawcy.

ZAMAWIAJĄCY:

WYKONAWCA:

* niepotrzebne skreślić

PROTOKÓŁ ODBIORU
do umowy nr podpisanej w dniu

Spisany pomiędzy stronami umowy:

Miastem i Gminą Bierutów z siedzibą w Bierutowie, przy ul. Moniuszki 12, **56-420 Bierutów NIP: 9111777417, w imieniu której działa Piotr Sawicki - Burmistrz Bierutowa, zwaną dalej: „Zamawiającym”,**

a

Firmą „Wykonawcą”.

PRZEDMIOT UMOWY:

1. **„Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”.**

W ramach działania cyfryzacji biur, jednostek publicznych, jednostek podległych i nadzorowanych:

Część nr 1 – Zakup serwerów*;

Część nr 2 – Modernizacja wewnętrznej sieci LAN*;

Część nr 3 – Zakup urządzenia wielofunkcyjnego z możliwością skanowania do sieci*;

Część nr 4 – Zakup oprogramowania biurowego*;

Część nr 5 – Zakup systemu do tworzenia kopii bezpieczeństwa*;

W ramach działania zapewnienie cyberbezpieczeństwa samorządowych systemów informatycznych:

Część nr 6 – Zakup oprogramowania do monitorowania urządzeń sieciowych*;

Część nr 7 – Zakup oprogramowania i urządzenia do ochrony brzegu sieci*.

2. Wykonawca przekazując niniejszy sprzęt oświadcza, że jest on nowy i spełnia parametry ujęte w umowie (jeśli dotyczy)*
3. Przekazywany sprzęt został sfinansowany 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, w ramach

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21.

Umowa o powierzenie grantu nr 2944/1/2021 z dnia 10.02.2022 r.

4. Wykonawca przekazuje następujący sprzęt/oprogramowanie*:

L.p.	Nazwa	Model sprzętu /Rodzaj oprogramowania	Numer seryjny/ Numer produktu	Ilość
1				
2				
3				
4				
5				
6				

* niepotrzebne skreślić

5. Zamawiający odbiera przedmiot umowy w całości/ w części.

6. Zamawiający zatwierdza do wypłaty kwotę:....., słownie:

.....

ZAMAWIAJĄCY:

WYKONAWCA:

**Załącznik Nr 6 do SIWZ -
Wzór umowy o powierzenie
przetwarzania danych osobowych**

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia 2022 r. pomiędzy:
(zwana dalej „Umową”)

Urzędem Miejskim w Bierutowie, ul. Moniuszki 12, 56 – 420 Bierutów

zwanym w dalszej części umowy „**Podmiotem przetwarzającym**”
reprezentowanym przez:

- Burmistrza Bierutowa – Piotra Sawickiego

oraz

firmą z siedzibą w
zarejestrowaną w Centralnej Ewidencji i Informacji Działalności Gospodarczej, NIP
..... lub w Krajowym Rejestrze Sądowym nr

zwaną w dalszej części umowy „**Administratorem danych**” lub
„Administratorem”

reprezentowaną przez.....

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu dane osobowe do przetwarzania, w trybie art. 28 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, zwanej dalej „RODO”, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi RODO.

§ 2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane w zakresie określonym w załączniku do niniejszej umowy.
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy nr 272/.../2022 z dnia r. na zadanie pn.: **Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”**.

§ 3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 RODO.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 lit. b RODO) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 RODO.

*niepotrzebne skreślić

7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu 24 h.

§ 4

Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 lit. h) RODO ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 3-dniowym jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.

§ 5

Dalsze powierzenie danych do przetwarzania

1. Administrator może powierzyć Podmiotowi przetwarzającemu dane osobowe podwykonawcy do dalszego przetwarzania jedynie w celu wykonania umowy .
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający.
W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na nim obowiązków ochrony danych podwykonawcy.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.

2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§ 7

Czas obowiązywania umowy

Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas wykonania przedmiotu umowy nr .../2022 z dnia r.

§ 8

Rozwiązanie umowy

Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:

- 1) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
- 2) przetwarza dane osobowe w sposób niezgodny z umową;
- 3) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§ 9

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż

wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla Podmiotu przetwarzającego.

PODMIOT PRZETWARZAJĄCY

ADMINISTRATOR DANYCH

Załącznik do umowy
POWIERZENIA PRZETWARZANIA
DANYCH OSOBOWYCH

Rejestr czynności przetwarzania danych osobowych

Nazwa czynności przetwarzania	Kategorie danych
Przetwarzanie danych osobowych zawartych w ofertach i dokumentacji wykonawców w związku z udzieleniem zamówienia publicznego	Dane identyfikacyjne, dane teleadresowe

Załącznik Nr 7 do SWZ –
ZOBOWIĄZANIE INNEGO PODMIOTU (jeśli dotyczy)

Nazwa zadania:

Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” Część nr 1*/ Część nr 2*/Część nr 3*/Część nr 4*/Część nr 5*/Część nr 6*/Część nr 7*

Uwaga: Niniejsze zobowiązanie wypełnia podmiot trzeci w przypadku, gdy wykonawca polega na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej podmiotów udostępniających zasoby w celu potwierdzenia spełniania warunków udziału w postępowaniu.

ZOBOWIĄZANIE PODMIOTU UDOSTĘPNIAJĄCEGO ZASOBY

Ja(My) niżej podpisany(i):

.....
(imię i nazwisko osoby upoważnionej do reprezentowania podmiotu udostępniającego zasoby)

działając w imieniu i na rzecz:

.....
(nazwa i adres podmiotu udostępniającego zasoby)

Zobowiązuję się, zgodnie z postanowieniami art. 118 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r., poz. 1129 ze zm.), do oddania nw. zasobów:

.....
(określenie zasobów)

do dyspozycji Wykonawcy:

.....
(nazwa i adres Wykonawcy składającego ofertę)

na potrzeby realizacji zamówienia pn. **Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”**

Oświadczam, że:

a) udostępnię Wykonawcy zasoby, w następującym zakresie:

.....

„Sfinansowano w ramach reakcji Unii na pandemię COVID-19”

b) sposób wykorzystania udostępnionych przeze mnie zasobów przy wykonywaniu zamówienia publicznego będzie następujący:

.....

c) zakres mojego udziału przy realizacji zamówienia publicznego będzie następujący:

.....

d) okres mojego udostępnienia zasobów Wykonawcy będzie następujący:

.....

Oświadczam, że jako podmiot udostępniający powyższe zasoby wezmę udziału w realizacji niniejszego zamówienia jako podwykonawca.

Podmiot, który zobowiązał się do udostępnienia zasobów, odpowiada solidarnie z Wykonawcą za szkodę Zamawiającego powstałą w skutek nie udostępnienia tych zasobów, chyba że za nieudostępnienie zasobów nie ponosi winy.

(Oświadczenie musi być opatrzone przez osobę lub osoby uprawnione do reprezentowania podmiotu udostępniającego zasoby kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. Oświadczenie należy złożyć wraz z ofertą)

Załącznik Nr 8 do SWZ –
Oświadczenie o grupie kapitałowej

Nazwa zadania:

Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” Część nr 1*/ Część nr 2*/Część nr 3*/Część nr 4*/Część nr 5*/Część nr 6*/Część nr 7*

Oświadczenie Wykonawcy

składane w zakresie art. 108 ust. 1 pkt. 5 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r., poz. 1129 ze zm.) (dalej jako: ustawa Pzp), dotyczące:

przynależności lub braku przynależności do grupy kapitałowej

Na potrzeby postępowania o udzielenie zamówienia publicznego pn.: **Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina”**

oświadczam/(-my), co następuje:

nie przynależę* do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r. poz. 275), z innym Wykonawcą, który złożył odrębną ofertę w niniejszym postępowaniu.

przynależę* do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r. poz. 275), z innym Wykonawcą, który złożył odrębną ofertę w niniejszym postępowaniu:

Lp	Nazwa podmiotu	Adres podmiotu
1		
2		

Uwaga:

Wykonawca może przedstawić dokumenty lub informacje potwierdzające przygotowanie oferty niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej.

* - niepotrzebne skreślić

(Oświadczenie musi być opatrzone przez osobę lub osoby uprawnione do reprezentowania Wykonawcy kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym. Oświadczenie należy złożyć po wezwaniu przez Zamawiającego)

Załącznik Nr 9 do SWZ –
Klauzula informacyjna

Nazwa zadania:

Zakup i dostawa sprzętu i oprogramowania w ramach projektu „Cyfrowa Gmina” Część nr 1*/ Część nr 2*/Część nr 3*/Część nr 4*/Część nr 5*/Część nr 6*/Część nr 7*

KLAUZULA INFORMACYJNA

Urząd Miejski w Bierutowie informuje, że:

- 1) Administratorem Pani/Pana danych osobowych jest **Burmistrz Bierutowa, wykonujący swoje zadania przy pomocy Urzędu Miejskiego w Bierutowie, zlokalizowanego w Bierutowie przy ul. Moniuszki 12;**
- 2) Przedstawicielem Administratora jest – **nie wyznaczono przedstawiciela** (tylko, jeśli ma zastosowanie – nazwisko, imię, pełniona funkcja przedstawiciela oraz jego dane kontaktowe)
- 3) **Inspektor Ochrony Danych Osobowych wykonuje swoje obowiązki w siedzibie Urzędu Miejskiego w Bierutowie, zlokalizowanego w Bierutowie przy ul. Moniuszki 12, Bud. A, pok. 7, tel.71 314 62 51 wew. 38, e-mail: iod@bierutow.pl;**
- 4) Pani/Pana dane osobowe będą przetwarzane **w celach** niezbędnych do realizacji umowy o powierzenie grantu nr 2944/1/2021 z dnia 10.02.2022 r. oraz do badania kwalifikowalności środków, udzielenia wsparcia, ewaluacji, monitoringu, kontroli, sprawozdawczości, itp. w Projekcie realizowanym przez Miasto i Gminę Bierutów, pn.: „Cyfrowa Gmina”, który finansowany jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, w ramach konkursu grantowego Cyfrowa Gmina o numerze POPC.05.01.00-00-0001/21-00
- 5) **Podstawą prawną przetwarzania dotyczących Pani/Pana danych osobowych jest:**
Artykuł 6. ust.1, pkt. b),c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/ 679 z dnia 27 kwietnia 2016r., w sprawie ochrony danych osób fi-

Zadanie pn.: „Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina” finansowane jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczy realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-0001/21-00

- zycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchyleni dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych „RODO”).
- 6) Odbiorcą Pani/Pana danych osobowych będzie – **dane będą przekazywane do:**
- Centrum Projektów polska cyfrowa , z siedzibą w Warszawie , 01-044, ul. Spokojna 13 A,
 - podmiotów, którym Instytucja Zarządzająca POPC 2014-2020 powierzyła wykonywanie zadań związanych z realizacją Programu, w tym w szczególności Instytucja Pośrednicząca POPC,
 - a także eksperci, podmioty prowadzące audyty, kontrole, szkolenia i ewaluacje,
 - instytucji, organów i agencji Unii Europejskiej (UE), a także innym podmiotom, którym UE powierzyła wykonywanie zadań związanych z wdrażaniem POPC 2014-2020,
- (dane odbiorcy, odbiorców lub kategorii odbiorców)
- 7) Pani/Pana dane będą przekazywane do państwa trzeciego, organizacji międzynarodowej – **dane nie będą przekazywane do państwa trzeciego.**
- 8) Okres przechowywania Pani/Pana danych osobowych upływa z:
Dane osobowe będą przechowywane przez okres wskazany w art. 140 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 z dnia 17 grudnia 2013 r. oraz jednocześnie przez czas nie krótszy niż 10 lat od dnia przyznania ostatniej pomocy w ramach POPC 2014-2020 - z równoczesnym uwzględnieniem przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.
- 9) Posiada Pani/Pan prawo żądania od Administratora: **sprostowania, ograniczenia przetwarzania, wniesienia sprzeciwu wobec takiego przetwarzania, usunięcia, przenoszenia danych.**
(sprostowania, ograniczenia przetwarzania, wniesienia sprzeciwu wobec takiego przetwarzania, usunięcia, przenoszenia danych – w zakresie dopuszczonym przepisami prawa krajowego, przy czym usunięcie i przenoszenie danych możliwe jest wyłącznie, gdy administrator przetwarza dane na podstawie innej niż obowiązek prawny ciążący na Administratorze)
- 10) Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego.
- 11) Podanie danych jest niezbędne do realizacji umowy o powierzenie grantu nr 2944/1/2021 z dnia 11.02.2022 r. (ustawowym, umownym)

- 12) W przypadku niepodania danych, nie będzie możliwe ~~otrzymywanie informacji o obowiązujących~~ wykonanie umowy o powierzenie grantu nr 2944/1/2021 z dnia 10.02.2022 r.
- 13) Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

OŚWIADCZENIE o wyrażeniu zgody na przetwarzanie danych osobowych

Wyrażam dobrowolną zgodę na przetwarzanie dotyczących mnie danych osobowych przez Administratora, którym jest Burmistrz Bierutowa, wykonujący zadania przy pomocy Urzędu Miejskiego w Bierutowie, zlokalizowanego w Bierutowie przy ul. Moniuszki 12, w zakresie - nazwa wykonawcy, imię, nazwisko, kraj, nip, adres: ulica, nr budynku, nr lokalu, kod pocztowy, miejscowość, nr rachunku bankowego, kwota wynagrodzenia

w celach niezbędnych do realizacji umowy o powierzenie grantu nr 2944/1/2021 z dnia 10.02.2022 r. oraz do badania kwalifikowalności środków, udzielenia wsparcia, ewaluacji, monitoringu, kontroli, sprawozdawczości, itp. w Projekcie realizowanym przez Miasto i Gminę Bierutów, pn.: „Cyfrowa Gmina”, który finansowany jest z Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, w ramach konkursu grantowego Cyfrowa Gmina o numerze POPC.05.01.00-00-0001/21-00

zgodnie z art. 7 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 (Dz. Urz. UE L 119) oraz przepisami krajowymi.