



Cyberbezpieczny Samorząd

**POSTĘPOWANIE O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO O WARTOŚCI ZAMÓWIENIA PONIŻEJ
KWOT OKREŚLONYCH W PRZEPISACH WYDANYCH NA PODSTAWIE ART. 3 USTAWY Z DNIA 11
WRZEŚNIA 2019 R. PRAWO ZAMÓWIEŃ PUBLICZNYCH**
(Dz. U. z 2024 poz. 1320 z późn. zm.- dalej jako ustawa P.z.p.)

Nazwa zadania Cyberbezpieczny Samorząd

Znak sprawy: ZP.271.10.2025

Nazwa Zamawiającego: Miasto i Gmina Gołańcz
NIP: 7661975765
Miejscowość: Gołańcz
Adres: ul. dr. P. Kowalika 2, 62-130 Gołańcz
Strona internetowa: <https://golancz.pl/>

ZATWIERDZIŁ:

/-/BURMISTRZ MIASTA I GMINY GOŁAŃCZ

inż. Robert Torz

**Wszelką korespondencję związaną z niniejszym postępowaniem należy składać
za pośrednictwem serwisu Platforma Zakupowa:**

<https://platformazakupowa.pl/transakcja/1179915>

UWAGA:

Niniejsza SWZ składa się z następujących części:

- Część I :** Informacja dla wykonawców wraz z załącznikami;
Część II: Projekt umowy;



Spis treści

I.	NAZWA ORAZ ADRES ZAMAWIAJĄCEGO, NUMER TELEFONU, ADRES POCZTY ELEKTRONICZNEJ ORAZ STRONY INTERNETOWEJ PROWADZONEGO POSTĘPOWANIA	5
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
III.	TRYB UDZIELENIA ZAMÓWIENIA	5
IV.	OZNACZENIE POSTĘPOWANIA	5
V.	OPIS PRZEDMIOTU ZAMÓWIENIA	5
VI.	TERMIN WYKONANIA ZAMÓWIENIA	36
VII.	PROJEKTOWANE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI TEJ UMOWY	36
VIII.	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	36
IX.	INFORMACJE O SPOSOBIE KOMUNIKOWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI W INNY SPOSÓB NIŻ PRZY UŻYCIU ŚRODKÓW KOMUNIKACJI ELEKTRONICZNEJ W PRZYPADKU ZAISTNIENIA JEDNEJ Z SYTUACJI OKREŚLONYCH W ART. 65 UST. 1, ART. 66 I ART. 69.....	39
X.	WSKAZANIE OSÓB UPRAWNIONYCH DO KOMUNIKOWANIA SIĘ Z WYKONAWCAMI.....	39
XI.	TERMIN ZWIĄZANIA OFERTĄ	39
XII.	OPIS SPOSOBU PRZYGOTOWANIA OFERTY	39
XIII.	SPOSÓB ORAZ TERMIN SKŁADANIA OFERT	41
XIV.	TERMIN OTWARCIA OFERT	41
XV.	PODSTAWY WYKLUCZENIA Z POSTĘPOWANIA	42
XVI.	SPOSÓB OBLICZENIA CENY	44
XVII.	OPIS KRYTERIÓW OCENY OFERT, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT	45
XVIII.	INFORMACJA O FORMALNOŚCIACH, JAKIE MUSZĄ ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO.....	46
XIX.	POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY	46
XX.	INFORMACJA O WARUNKACH UDZIAŁU W POSTĘPOWANIU	47
XXI.	WYKAZ OŚWIADCZEŃ I DOKUMENTÓW SKŁADANYCH WRAZ Z FORMULARZEM OFERTOWYM	47



Cyberbezpieczny Samorząd

XXII.	INFORMACJA O PODMIOTOWYCH ŚRODKACH DOWODOWYCH - OŚWIADCZENIA I DOKUMENTY, JAKIE ZOBOWIĄZANI SĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ WYKAZANIA BRAKU PODSTAW WYKLUCZENIA . 48
XXIII.	INFORMACJA DLA WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA (SPÓŁKI CYWILNE/ KONSORCJA) 49
XXIV.	OPIS CZĘŚCI ZAMÓWIENIA 50
XXV.	LICZBA CZĘŚCI ZAMÓWIENIA, NA KTÓRĄ WYKONAWCA MOŻE ZŁOŻYĆ OFERTĘ, MAKSYMALNA LICZBA CZĘŚCI, NA KTÓRE ZAMÓWIENIE MOŻE ZOSTAĆ UDZIELONE TEMU SAMEMU WYKONAWCY, ORAZ KRYTERIA /ZASADY, MAJĄCE ZASTOSOWANIE DO USTALENIA, KTÓRE CZĘŚCI ZAMÓWIENIA ZOSTANĄ UDZIELONE JEDNEMU WYKONAWCY, W PRZYPADKU WYBORU JEGO OFERTY W WIĘKSZEJ NIŻ MAKSYMALNA LICZBIE CZĘŚCI 50
XXVI.	INFORMACJA DOTYCZĄCA OFERT WARIANTOWYCH, W TYM INFORMACJA O SPOSOBIE PRZEDSTAWIANIA OFERT WARIANTOWYCH ORAZ MINIMALNE WARUNKI, JAKIM MUSZĄ ODPOWIEDZIEĆ OFERTY WARIANTOWE 50
XXVII.	WYMAGANIA W ZAKRESIE ZATRUDNIENIA NA PODSTAWIE STOSUNKU PRACY, W OKOLICZNOŚCIACH, O KTÓRYCH MOWA W ART. 95 50
XXVIII.	WYMAGANIA W ZAKRESIE ZATRUDNIENIA OSÓB, O KTÓRYCH MOWA W ART. 96 UST. 2 PKT 2 50
XXIX.	INFORMACJA O ZASTRZEŻENIU MOŻLIWOŚCI UBIEGANIA SIĘ O UDZIELENIE ZAMÓWIENIA WYŁĄCZNIE PRZEZ WYKONAWCÓW, O KTÓRYCH MOWA W ART. 94 50
XXX.	WYMAGANIA DOTYCZĄCE WADIUM, W TYM JEGO KWOTA 51
XXXI.	INFORMACJA O PRZEWIDYWANYCH ZAMÓWIENIACH, O KTÓRYCH MOWA W ART. 214 UST. 1 PKT 7 I 8 51
XXXII.	INFORMACJA DOTYCZĄCA PRZEPROWADZENIA PRZEZ WYKONAWCĘ WIZJI LOKALNEJ LUB SPRAWDZENIA PRZEZ NIEGO DOKUMENTÓW NIEZBĘDNYCH DO REALIZACJI ZAMÓWIENIA, O KTÓRYCH MOWA W ART. 131 UST. 2 51
XXXIII.	INFORMACJA DOTYCZĄCA WALUT OBCYCH, W JAKICH MOGĄ BYĆ PROWADZONE ROZLICZENIA MIĘDZY ZAMAWIAJĄCYM A WYKONAWCĄ .. 51
XXXIV.	INFORMACJA DOTYCZĄCA ZWROTU KOSZTÓW UDZIAŁU W POSTĘPOWANIU 51
XXXV.	INFORMACJA O OBOWIĄZKU OSOBISTEGO WYKONANIA PRZEZ WYKONAWCĘ KLUCZOWYCH ZADAŃ ZGODNIE Z ART. 60 I ART. 121..... 51
XXXVI.	MAKSYMALNA LICZBA WYKONAWCÓW, Z KTÓRYMI ZAMAWIAJĄCY ZAWRZE UMOWĘ RAMOWĄ..... 52
XXXVII.	INFORMACJA O PRZEWIDYWANYM WYBORZE NAJKORZYSTNIEJSZEJ OFERTY Z ZASTOSOWANIEM AUKCJI ELEKTRONICZNEJ WRAZ Z INFORMACJAMI, O KTÓRYCH MOWA W ART. 230 52



Cyberbezpieczny Samorząd

XXXVIII.	WYMÓG LUB MOŻLIWOŚĆ ZŁOŻENIA OFERT W POSTACI KATALOGÓW ELEKTRONICZNYCH LUB DOŁĄCZENIA KATALOGÓW ELEKTRONICZNYCH DO OFERTY, W SYTUACJI OKREŚLONEJ W ART. 93.....	52
XXXIX.	INFORMACJA DOTYCZĄCA ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY.....	52
XL.	OBOWIĄZEK INFORMACYJNY WYNIKAJĄCY Z ART. 13 RODO W PRZYPADKU ZBIERANIA DANYCH OSOBOWYCH BEZPOŚREDNIO OD OSOBY FIZYCZNEJ, KTÓREJ DANE DOTYCZĄ, W CELU ZWIĄZANYM Z POSTĘPOWANIEM O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO	52
ZAŁĄCZNIKI DO CZĘŚCI I – SWZ - INTEGRALNĄ CZĘŚĆ NINIEJSZEJ SWZ STANOWIĄ WZORY NASTĘPUJĄCYCH DOKUMENTÓW:.....		53



CZĘŚĆ I INFORMACJA DLA WYKONAWCÓW WRAZ Z ZAŁĄCZNIKAMI

I. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO, NUMER TELEFONU, ADRES POCZTY ELEKTRONICZNEJ ORAZ STRONY INTERNETOWEJ PROWADZONEGO POSTĘPOWANIA

Nazwa Zamawiającego:	Miasto i Gmina Gołańcz
REGON:	000570791313
NIP:	766-19-75-765
Adres:	ul. Doktora Piotra Kowalika 2, 62-130 Gołańcz
Telefon:	+48 (67) 26-15-911
Adres poczty elektronicznej:	przetargi@golancz.pl
Adres strony internetowej prowadzonego postępowania:	https://platformazakupowa.pl/transakcja/1179915

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

<https://platformazakupowa.pl/transakcja/1179915>

inaczej strona internetowa prowadzonego postępowania

III. TRYB UDZIELENIA ZAMÓWIENIA

1. Postępowanie o udzielenie zamówienia prowadzone jest w **trybie podstawowym określonym w przepisach art. 275 pkt 1 ustawy P.z.p.**, tj. Zamawiający wybiera najkorzystniejszą ofertę bez przeprowadzenia negocjacji.
2. Szacunkowa wartość przedmiotowego zamówienia nie przekracza progów unijnych o jakich mowa w art. 3 ustawy P.z.p.

IV. OZNACZENIE POSTĘPOWANIA

Postępowanie oznaczone jest znakiem: **ZP 271.10.2025** Wykonawcy powinni we wszelkich kontaktach z Zamawiającym powoływać się na wyżej podane oznaczenie.

V. OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa i wdrożenie oprogramowania oraz sprzętu informatycznego zgodnie z poniższym zestawieniem w ramach projektu pn.: „Cyberbezpieczny Samorząd. Przewidywany termin realizacji właściwego zamówienia w przypadku dostaw zostanie określony na 50 dni od dnia zawarcia umowy. Wszelkie licencje na oprogramowanie muszą być dostarczone z wsparciem producenta, liczonym od daty zakończenia wdrożenia do 30.06.2026 r.

Przedmiot zamówienia otrzymał dofinansowanie w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC). Celem tego programu jest wzmocnienie krajowego systemu cyberbezpieczeństwa, w szczególności poprzez zwiększenie poziomu bezpieczeństwa informacji w jednostkach samorządu terytorialnego. Numer umowy FERC.02.02-CS.01-001/23/2385.

1.2. Wymagania ogólne



Cyberbezpieczny Samorząd

1. Wykonawca dostarczy urządzenia na swój koszt i ryzyko do siedziby urzędu tj. ul. Doktora Piotra Kowalika nr 2, 62-130 Gołańcz. Przez termin dostawy rozumie się dzień, w którym Wykonawca dostarczy Zamawiającemu ostatnie z urządzeń wchodzących w skład przedmiotu zamówienia, wolne od wad.
2. Na Wykonawcy ciąży odpowiedzialność z tytułu uszkodzenia lub utraty przedmiotu umowy, aż do chwili podpisania protokołu przekazania przez Zamawiającego.
3. Elementy składowe zestawów muszą być ze sobą kompatybilne, zapewnić bezproblemową współpracę, posiadać niezbędne elementy umożliwiające pracę urządzeń (w tym okablowanie).
4. Wykonawca zobowiązuje się dostarczyć przedmiot umowy fabrycznie nowy, bez wad wraz z aktualnymi atestami i certyfikatami bezpieczeństwa oraz wymaganiami norm.
5. Wykonawca dostarczy najpóźniej w dniu odbioru przedmiotu zamówienia dokumentację techniczną na przedmioty: opis techniczny urządzeń, karty gwarancyjne, dokumenty potwierdzające zgodność urządzeń z normami jakościowymi i specyfikacją, instrukcje obsługi w języku polskim itp.
6. Zamawiający wymaga, aby dostarczany system operacyjny był fabrycznie nowy, nieużywany oraz nigdy wcześniej nieaktywowany na innym urządzeniu. Zamawiający wymaga, aby system operacyjny był zainstalowany (lub preinstalowany) fabrycznie na komputerach. Zamawiający wymaga, aby system operacyjny był dostarczony wraz ze stosownymi, oryginalnymi atrybutami legalności, np. certyfikatami autentyczności. Zamawiający nie dopuszcza rozwiązań licencyjnych wymagających stałych opłat w okresie użytkowania systemu operacyjnego.
7. Podane w zestawieniu przedmiotów zamówienia opisy, czy parametry techniczne należy traktować, jako minimalne. Przedmioty opisane przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę można zastąpić innymi równoważnymi dostępnymi w handlu posiadającym takie same lub lepsze cechy użytkowe (funkcjonalne) niż wymienione w specyfikacji.
8. Wykonawca udzieli na dostarczony przedmiot zamówienia gwarancji jakości i rękojmi za wady. Warunki dotyczące gwarancji i rękojmi szczegółowo zostały określone w projektowanych postanowieniach umowy.
9. W cenie jednostkowej Wykonawca uwzględni w szczególności: kompletny przedmiot zamówienia, dostawę, transport, załadunek i rozładunek, serwis gwarancyjny oraz inne koszty wynikające ze specyfiki zamówienia.
10. W tabeli zestawienia przedmiotów w jednostce miary dla poszczególnych przedmiotów Zamawiający uwzględnił wszystkie artykuły określone w konkretnej pozycji opisu przedmiotu zamówienia.

1.3. Minimalne wymagania techniczne dotyczące przedmiotów:

Kody CPV:

48820000-2 – Serwery

30211400-5 – Konfiguracje komputerowe

48823000-3 – Serwery plików

48822000-6 – Serwery komputerowe

Opis przedmiotu zamówienia



Cyberbezpieczny Samorząd

Przedmiotem zamówienia jest dostawa i wdrożenie rozwiązań serwerowo-sieciowych wraz z oprogramowaniem współtowarzyszącym w Urzędzie Miasta i Gminy Gołańcz zgodnie z poniższą specyfikacją wraz z zapewnieniem wsparcia technicznego do czasu upływu gwarancji dostarczonej przez producenta sprzętu. Wdrożenie dostarczonego sprzętu teleinformatycznego wraz oprogramowaniem współtowarzyszącym ma obejmować:

- Kompleksową instalację i uruchomienie dostarczonego sprzętu w siedzibie Zamawiającego w miejscu (serwerowni) przez Niego wskazanym zgodnie z procedurami przewidzianymi przez producenta.
- Konfigurację oprogramowania preinstalowanego na dostarczonych urządzeniach zgodnie z przewidzianą procedurą/schematem postępowania przez producenta tak aby urządzenie/oprogramowanie korelowało z uwarunkowanymi techniczno-środowiskowymi sieci teleinformatycznej Zamawiającego.
- Instalację i konfigurację dodatkowych systemów/oprogramowania na dostarczonych urządzeniach ujętych w opisie przedmiotu zamówienia.
- Wdrożenie i przeszkolenie pracownika obsługi informatycznej Zamawiającego z obsługi dostarczonych urządzeń oraz oprogramowania.
- Opracowanie i przekazanie dokumentacji powdrożeniowej(uruchomieniowej) dostarczonych urządzeń/oprogramowania wraz z kopiami konfiguracyjnymi w formie cyfrowej.
- Zapewnienie wsparcia merytorycznego na czas trwania projektu tj. do 30.06.2026 r.

Serwer wraz z systemem operacyjnym oraz licencjami dostępowymi dla użytkowników – 2 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 1U z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 32 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	• Zainstalowane dwa procesory min. 8-rdzeniowe (każdy) , min. 2.9GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 175 pkt w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	• Minimum 256GB DDR5 RDIMM 5600MT/s, • Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.



Cyberbezpieczny Samorząd

Funkcjonalność pamięci RAM	• Demand Scrubbing, • Patrol Scrubbing, • Permanent Fault Detection
Gniazda PCI	• minimum dwa sloty PCIe w tym jeden generacji 5
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Dyski twarde	• Zainstalowane dwa dyski M.2 SSD samoszyfrujące o pojemności min. 480GB z możliwością konfiguracji RAID 1.
Wbudowane porty	• 4 x USB z czego nie mniej niż 1x USB 3.0, 2x VGA
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	• Redundantne, Hot-Plug min. 1100W każdy o efektywności min. 90% w pełnym zakresie obciążenia
Bezpieczeństwo	• Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • 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
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ○ szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; ○ możliwość podmontowania zdalnych wirtualnych napędów; ○ wirtualną konsolę z dostępem do myszy, klawiatury; ○ wsparcie dla IPv6; ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ○ integracja z Active Directory; ○ możliwość obsługi przez dwóch administratorów jednocześnie; ○ wsparcie dla dynamic DNS; ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.



Cyberbezpieczny Samorząd

	- o możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera - o możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: - o Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej - o Przesyłanie danych telemetrycznych w czasie rzeczywistym - o Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze - o Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: - o Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych - o integracja z Active Directory - o Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta - o Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish - o Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram - o Szczegółowy opis wykrytych systemów oraz ich komponentów - o Możliwość eksportu raportu do CSV, HTML, XLS, PDF - o Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. - o Grupowanie urządzeń w oparciu o kryteria użytkownika - o Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji - o Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach - o Szybki podgląd stanu środowiska - o Podsumowanie stanu dla każdego urządzenia - o Szczegółowy status urządzenia/elementu/komponentu - o Generowanie alertów przy zmianie stanu urządzenia. - o Filtry raportów umożliwiające podgląd najważniejszych zdarzeń - o Integracja z service desk producenta dostarczonej platformy sprzętowej - o Możliwość przejęcia zdalnego pulpitu - o Możliwość podmontowania wirtualnego napędu - o Kreator umożliwiający dostosowanie akcji dla wybranych alertów - o Możliwość importu plików MIB - o Przesyłanie alertów „as-is” do innych konsol firm trzecich - o Możliwość definiowania ról administratorów - o Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów - o Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) - o Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta - o Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów



Cyberbezpieczny Samorząd

	- o Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. - o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. - o Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile - o Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. - o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. - o Zdalne uruchamianie diagnostyki serwera. - o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. - o Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
System operacyjny	• Ze względu na potrzebę zachowania kompatybilności ze stosowanym obecnie przez Zamawiającego oprogramowaniem wymagane jest dostarczenie wraz z serwerem bezterminowej, nowej (nieaktywowanej wcześniej) licencji na oprogramowanie MS Windows Server 2025 Standard pozwalającej na uruchomienie na każdym z zaoferowanych serwerów min. 4 instancji środowiska wirtualnego MS Windows Server 2025 Standard oraz min. 100 bezterminowych licencji MS Windows Server 2025 UserCAL do w/w środowiska.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży z ofertą dokument potwierdzający spełnianie wymogu.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Gwarancji producenta: min. 3 lata • Możliwość rozszerzenia gwarancji przez producenta do 7 lat.



Cyberbezpieczny Samorząd

	• Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. • Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. • 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 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość rozszerzenia gwarancji o: • Wyznaczonego przez wykonawcę Opiekuna Technicznego Klienta, do którego obowiązków będzie należało: ○ Monitorowanie zdarzeń w obrębie infrastruktury ○ Zarządzanie eskalacjami i współpraca z kierownikiem eskalacji • Przygotowywanie kwartalnych zaleceń dotyczące konserwacji infrastruktury sprzętowej (BIOS, firmware, patche) • Zdalne lub na miejscu wdrażanie poprawek - 2x w roku • Raportowanie realizacji kontraktów serwisowych i wykorzystania zasobów sprzętowych (na żądanie)
--	---



Macierz dyskowa – 1 szt.

Macierz dyskowa w konfiguracji:			
Lp.	Nazwa parametru	Minimalna wartość parametru	Komentarz
	Obudowa i komponenty	System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19". Podzespoły macierzy tj. wentylatory, zasilacze muszą być w pełni redundantne, żeby zapewnić odpowiedni poziom bezpieczeństwa.	
2.	Pojemność:	System musi zostać dostarczony w konfiguracji zawierającej minimum: 8 dysków 1,9TB NVME oraz posiadać możliwość rozbudowy o kolejne dyski. Przestrzeń powinna być zarządzana przez dwa kontrolery w momencie dostawy. System musi wspierać dyski o wielkościach: ■ NVME: do wielkości co najmniej 15,3TB	
3.	Kontroler	Dwa kontrolery wyposażone w przynajmniej 64GB cache każdy. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania baterijnego przez minimum 72 godziny lub za pomocą zrzutu danych na pamięć nie ulotną. Ze względu na kompatybilność z infrastrukturą zamawiającego procesory macierzy muszą być wykonane w technologii INTEL lub AMD wielordzeniowej. Macierz musi pozwalać na rozbudowę do klastra 24	



Cyberbezpieczny Samorząd

		kontrolerów lub musi pozwalać na obsługę przynajmniej 1152 dysków w obrębie pary kontrolerów lub klastra w szczególności rozbudowę w technologii NVMe z obsługą min 1152 dysków w technologii NVME.	
4.	Interfejsy	Oferowana macierz musi posiadać minimum: ▪ 8 portów 10/25GbE - każdy port obsadzony wkładkami producenta macierzy co najmniej o prędkości 25Gb ▪ 4 porty 1Gb RJ45 (2x port do zarządzania + 2x Port konsolowy) Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+), zamawiający wymaga ich dostarczenia wraz z urządzeniem.	
5.	RAID	System RAID musi zapewniać taki poziom zabezpieczania danych, aby był możliwy do nich dostęp w sytuacji awarii minimum dwóch dysków w grupie RAID	
6.	Kopie Migawkowe	Macierz musi być wyposażona w system kopii migawkowych, dostępny dla wszystkich rodzajów danych przechowywanych na macierzy. System kopii migawkowych nie może powodować spadku wydajności macierzy +/-5%.	
7.	Obsługiwane protokoły	Macierz musi obsługiwać jednocześnie protokoły FC; iSCSI; NFS; pNFS; NVMe/FC; NVMe/TCP; CIFS/SMB, S3 Zamawiający w tym postępowaniu wymaga dostarczenia licencji na wszystkie protokoły.	
8.	Inne wymagania	Macierz musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych in-line. Macierz musi posiadać także funkcjonalność kompresji danych in-line.	



Cyberbezpieczny Samorząd

		Jeżeli oferowane rozwiązanie nie pozwala na deduplikację i kompresję w locie lub nie posiada możliwości deduplikacji i kompresji zamawiający wymaga dostarczenie 4 krotnej pojemności wyspecyfikowanej w punkcie 2. Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Win 2003/2008, Linux, Vmware, Unix Macierz musi posiadać funkcjonalność priorytetyzacji zadań w tym ustawienie max parametrów (I/Ops i Mbps) dla poszczególnych LUN. Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie. Macierz musi posiadać funkcjonalność replikacji danych z inną macierzą tego samego producenta w trybie synchronicznym i asynchronicznym. Funkcjonalność replikacji danych musi być natywnym narzędziem macierzy. Przed procesem replikacji macierz musi umożliwiać włączenie procesu deduplikacji danych i kompresji danych w celu optymalizacji wykorzystania łącza dla replikowanych zasobów lub zamawiający wymaga dostarczenia zewnętrznego narzędzia do deduplikowania replikowanych danych lub dwukrotnego zwiększenia pojemności ze względu na rozważaną w przyszłości replikację całości zasobów.	
--	--	---	--



Cyberbezpieczny Samorząd

		Macierz musi posiadać funkcjonalność klonowania danych bez potrzeby fizycznego kopiowania danych na nośnikach. Macierz musi posiadać funkcjonalność wykonania spójnego snapshotu dla następujących aplikacji: - VMware - SAP - Oracle - MS Exchange oraz MS SQL - Veeam Oferowana konfiguracja macierzy musi pozwalać na osiągnięcie wydajności min 205 000 IOPS przy 8Kb bloku i stosunku 70/30% odczyt/zapis. Wydajność musi być osiągnięta przy uruchomionych technologiach efektywnego wykorzystania przestrzeni deduplikacja oraz kompresja jednocześnie, przy opóźnieniach średnich 1ms. Zamawiający wraz z ofertą wymaga dostarczenia oficjalnego dokumentu producenta z wymiarowaniem wydajności oraz dopuszcza możliwość sprawdzenia wydajności macierzy przy odbiorze. Macierz musi posiadać narzędzie umożliwiające generowanie raportu o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne macierzy. Macierz musi być wyposażona oprogramowanie do audytu zasobów plikowych w szczególności pozwalając na: - blokowanie zapisywania plików z określonym (do	
--	--	--	--



Cyberbezpieczny Samorząd

		zdefiniowania przez administratora) rozszerzeniem - monitorowaniu operacji wykonywanych na plikach Macierz musi posiadać dodatkowe lub wbudowane narzędzie pozwalające na ochronę przed złośliwym oprogramowaniem na zasobach plikowych, oprogramowanie musi pozwalać na analizę zachowań użytkowników oraz systemu i na tej podstawie pozwalać na wykrywanie anomalii wskazujących na aktywność złośliwego oprogramowania. Oprogramowanie musi pozwalać na wykrycie anomalii, poinformowanie administratora i zainicjowanie kopii typu snapshot. Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy. Z macierzą zamawiający wymaga dostarczenia oprogramowania które pozwala na: - monitoring wykorzystania przestrzeni na macierzy - monitoring grup RAIDowych - monitoring wykonywanych backupów/replikacji danych między macierzami - monitoring wydajności macierzy - analizę i diagnozę spadku wydajności Zamawiający dopuszcza zastosowanie oprogramowania zewnętrznego, na pełną max pojemność systemu. Macierz musi posiadać funkcjonalność „Tieringu” zimnych danych na: - inną macierz tego samego producenta (z wolnymi dyskami np. NL-SAS)	
--	--	---	--



Cyberbezpieczny Samorząd

		- inną macierz dowolnego producenta z protokołem S3 Tiering musi być natywnym narzędziem macierzy i wykonywać się automatycznie. Producent macierzy musi znajdować się w śród liderów „Leader” w raporcie Gartnera dla rozwiązań Storage przynajmniej dwóch poprzednich latach. Oferowane rozwiązanie musi obsługiwać możliwość stworzenia konfiguracji klastra geograficznego. Przez klaster geograficzny zamawiający rozumie automatyczne przełączanie zasobów z jednej macierzy dwukontrolerowej na inną macierz dwukontrolerową w trybie: - bez ingerencji inżyniera (Automatic Failover) - z ingerencją inżyniera (Manual Failover) Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność urządzenia i pozwalać na wspólne działanie (żadna funkcjonalność nie może wykluczać działania innej funkcjonalności).	
9.	Gwarancja i serwis	3 lata serwisu producenta i dostawą części na następny dzień roboczy po diagnozie problemu. Dostarczony serwis musi umożliwiać zgłaszanie awarii w trybie 24x7. W przypadku awarii dysku uszkodzony nośnik pozostaje własnością Zamawiającego. Dostarczony system musi posiadać również 3 lata subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych	



Cyberbezpieczny Samorząd

		dotyczących oferowanego urządzenia.	
10.	Dodatkowa funkcjonalność	Zamawiający wymaga, aby istniała możliwość instalacji wirtualnej wersji systemu operacyjnego macierzy w formie SDS (Software Defined Storage) na platformie wirtualizacyjnej: Vmware, MS Hyper-V, XEN lub KVM. Wirtualna wersja macierzy uruchomiona w ten sposób musi mieć możliwość replikacji z fizyczną macierzą wyspecyfikowaną przez zamawiającego. Replikacja musi odbywać się natywnymi mechanizmami macierzy. Replikacja musi być możliwa do uruchomienia w obu kierunkach z zachowaniem wykonanych operacji oszczędzających przestrzeń tj. deduplikacja. Transfer między fizycznym systemem, a jego wirtualną instancją będzie realizowany tylko przyrostowo. Zamawiający wymaga, aby zaoferowane urządzenia były uznanymi rozwiązaniami na świecie – producent zaoferowanego rozwiązania musi być notowany w raportach Gartnera dla rozwiązań "Primary Storage" nie starszych niż 3 lata przed złożeniem oferty i być wymieniony w grupie liderów (ang. Leaders). Jako równoważny dla raportu Gartnera Zamawiający dopuści również inny raport udostępniany publicznie, powszechnie akceptowany, mający charakter zewnętrznego i obiektywnego raportu standaryzacyjnego, który zapewnia analizę, wgląd w kierunek oraz dojrzałość uczestników rynku w rozwiązaniach typu Primary	



Cyberbezpieczny Samorząd

		Storage, aktualizowany co roku od min. 20 lat	
--	--	--	--

Przełączniki sieciowe – 4 szt.

W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymagany jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa, o następujących parametrach:

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Maksymalny pobór mocy: 60 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

1. Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
 - a) 48 porty GE RJ-45.
 - b) 4 porty 10 GE SFP+.

Zarządzanie

- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.



Cyberbezpieczny Samorząd

- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
 - Centralne zarządzanie konfiguracją urządzenia
 - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
 - Centralne zarządzanie sieciami VLAN.
 - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
 - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
 - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
 - Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
 - Automatyczna detekcja i rekomendacje konfiguracji.
 - Przesyłanie logów na zewnętrzny serwer syslog.
 - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
 - Obsługa białych i czarnych list adresów MAC.
 - Wykrywanie aplikacji komunikujących się w sieci.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres min. 24 m-cy 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.
2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.



Cyberbezpieczny Samorząd

Rozwiązania zasilania awaryjnego - UPS– 1 szt.

Zasilacz UPS do serwerów		
1	Moc pozorna	Min. 5000VA
2	Moc czynna	Min. 4500W
3	Architektura UPS-a	Online, podwójna konwersja, pełna sinusoida
4	Liczba faz na wejściu	1
5	Liczba zestawów akumulatorów	1
6	Czas podtrzymania (obciążenie 100%)	min. 3,5 min.
7	Typ obudowy	Rack 19" 3U
8	Funkcje specjalne	AVR
9	Ochrona przed przepięciami	Min. 470 J
10	Stopień ochrony	Min. IP20
11	Porty zasilania wyjściowe	Min. 5 x IEC C13 Min. 4 x IEC C19
12	Interfejsy:	Karta do zarządzania Web SNMP Management Card z czujnikami środowiskowymi
13	Wymiary: suma wymiarów szer/dł/wys	Maks. 130cm
14	Waga:	Maks. 55 kg
15	Certyfikaty	CE
16	Gwarancja producenta:	min. 36 m-cy na urządzenie i 24 m-ce na baterię.
17	Oprogramowanie do zarządzania	Zgodność (pełna funkcjonalność) z aktualnie posiadanym przez Zamawiającego oprogramowaniem APC PowerChute

System do gromadzenia i analizy zapisów działań w systemach wraz ze wsparciem na czas trwania projektu – 1 szt.

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

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

Interfejsy, Dysk:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

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

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.



Cyberbezpieczny Samorząd

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

Raportowanie

W zakresie raportowania system musi zapewniać:

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

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
 - Malware.
 - Aplikacje sieciowe.
 - Email.
 - IPS.
 - Traffic.
 - Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.



Cyberbezpieczny Samorząd

5. Funkcję zarządzania zdarzeniami z automatyzacją zadań, która może być konfigurowalna za pomocą playbooków składających się z reakcji i sekwencji zautomatyzowanych działań.
6. Funkcję, która umożliwia administratorom wyświetlanie alertów typu Outbreak i automatyczne pobieranie powiązanych zdarzeń oraz raportów od producenta rozwiązania.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
 - a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy i licencje

1. Licencja na system musi być ważna do 30.06.2026 r. oraz upoważniać do aktualizacji oprogramowania oraz wsparcia technicznego producenta w trybie 24x7.

System kopii Zapasowych – 1 szt.

Oprogramowanie musi umożliwiać wykonywanie kopii zapasowych min. 10 maszyn wirtualnych uruchomianych w środowisku Zamawiającego.

Zamawiający wymaga aby oprogramowanie było objęte wsparciem technicznym producenta oprogramowania (wraz z prawem do używania najnowszej wersji oprogramowania) na okres do 30.06.2026 r.

Wymagania ogólne

Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner Peer Insights: i spełniać minimalne wymaganie: - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,

Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej

Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.5.x - 7.0, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.4 lub nowszy oraz Proxmox VE 8.2 lub nowszy.

Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Całkowite koszty posiadania



Cyberbezpieczny Samorząd

Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla conajmniej trzech pamięci masowych to takiej puli.
Oprogramowanie musi pozwalać na przechowywanie kopii bezpieczeństwa w chmurze producenta.
Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
Oprogramowanie musi wspierać niezmiennność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora)
Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS)
Oprogramowanie musi posiadać integracje z systemami typu SIEM



Cyberbezpieczny Samorząd

Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.
<u>Wymagania RPO</u>
Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna conajmniej dla platformy VMware i Hyper-V
Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.
Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).
Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAAI, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.
Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
<u>Wymagania RTO</u>
Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.



Cyberbezpieczny Samorząd

Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere
Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
Oprogramowanie musi pozwalać na backup i odtwarzanie usługi Entra ID. W szczególności użytkowników, grupy, role, jednostki administracyjne, enterprise applications oraz logi audytowe i sign-in.
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.



Cyberbezpieczny Samorząd

Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2
Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
<u>Ograniczenie ryzyka</u>
Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych
Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
Oprogramowanie musi posiadać swój wbudowany program antywirusowy zoptymalizowany do przeszukiwania kopii backupowych
Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware
Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania
Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków
Oprogramowanie musi posiadać mechanizm wykrywania oznak ataku hakerskiego tzw Indicators of Compromise
Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.



Cyberbezpieczny Samorząd

Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR
<u>Środowiska fizyczne</u>
Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE, Rocky Linux, AlmaLinux
Rozwiązanie musi wspierać system operacyjny macOS
Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
Rozwiązanie musi wspierać backup podłączonych dysków USB
Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)
Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
Rozwiązanie musi wspierać kontrolę pasma sieciowego
Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
Rozwiązanie musi wspierać technologię BitLocker
Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednorazowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów baz danych
Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle i PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform



Rozwiązanie musi wspierać szyfrowanie
Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
Monitoring
System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.



System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware
<u>Raportowanie</u>
System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware
System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie



Cyberbezpieczny Samorząd

Wymagania dla przestrzeni obiektowej

Rozwiązanie musi oferować przestrzeń obiektową w chmurze na przechowywanie danych kopii zapasowych o pojemności min. 5TB

Rozwiązanie musi posiadać możliwość dodania repozytorium bezpośrednio z interfejsu oprogramowania backupowego zaoferowanego rozwiązania do wykonywania kopii zapasowych

Rozwiązanie musi być rozliczane poprzez jedną opłatę za okres min. do 30.06.2026 r. z wliczoną ceną na operacje odczytywanie/odtworzenie danych dla co najmniej 20% zaoferowanej pojemności.

Rozwiązanie musi posiadać mechanizmy wysokiej dostępności w ramach pojedynczej strefy dostępności.

Rozwiązanie musi być oparte o przechowywanie danych backupu w zapewniającej najwyższe standardy chmurze o zasięgu globalnym tj. której ośrodki przetwarzania i przechowywania danych znajdują się w minimum 3 krajach UE.

Wymagania sprzętowe

Specyfikacja sprzętowa	
Procesor	Procesor 64-bitowy x86 osiągający w teście PassMark Performance Test, co najmniej 27 000 punktów w kategorii Average CPU Mark, o taktowaniu nie mniejszym niż 5.1 GHz
Zainstalowana pamięć RAM	Min. 16 GB ECC DDR5, możliwość rozbudowy do 192 GB
Pamięć Flash	Min. 5 GB
Liczba zatok na dyski	Min.14, w tym min. 12 x 3,5-calowych SATA oraz min. 2 x M.2 2280 NVMe
Obsługiwane dyski twarde	3.5" SATA , 2.5" SATA oraz M.2 NVMe SSD
Zainstalowane dyski twarde	Min. 12 szt. dysków o pojemności min. 12TB 7200 obr/min dedykowanych do pracy w urządzeniu typu NAS. Dyski muszą znajdować się na liście kompatybilności publikowanej przez producenta urządzenia.
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 GbE	Min. 2 szt.
Porty LAN 10 GbE	Min. 2 szt.
Porty USB 3.2 Gen2	Min. 2 szt.
Port PCIe	Min. 3 szt.
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, 2U
Zasilanie	Zasilacz redundantny, max 550W
Specyfikacja oprogramowania	
Obsługa dwóch systemów operacyjnych	Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT
Szyfrowanie udziałów	Tak, min AES 256



Cyberbezpieczny Samorząd

Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Poziomy RAID: Pojedynczy Dysk, 0, 1, 5, 6, 10, 50, 60, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediiów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP, OpenVPN



Cyberbezpieczny Samorząd

Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Warunki gwarancji	Wymagane min. 3 lata gwarancji producenta urządzenia. W przypadku awarii dysków uszkodzone nośniki danych pozostają u Zamawiającego.

Zakup systemu zabezpieczającego przed wyciekiem danych z organizacji – 1 szt.

System DLP dla 50 stanowisk spełniający następujące wymagania minimalne:

Licencja wieczysta z wsparciem technicznym producenta do 30.06.2026 r.

- Obsługiwane systemy operacyjne – klient:
 - Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
 - Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
 - MacOS 12 lub nowszy.
- Serwer administracyjny musi obsługiwać instalację na systemach:



Cyberbezpieczny Samorząd

- a. Windows Server 2016 (64-bit) i nowszych.
3. Serwer administracyjny musi obsługiwać bazy danych:
 - a. MS SQL Server 2016 lub nowsze
 - b. MS SQL Express
 - c. AzureSQL S3 lub nowsze.
4. Pomoc i dokumentacja programu dostępne w języku angielskim.
5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
7. Serwer administracyjny musi umożliwiać instalację/deinstalację zdalnego klienta na stacjach roboczych.
8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
11. System musi posiadać mechanizm usuwający najstarsze informacje, gdy rozmiar bazy osiągnie domyślny limit.
12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.
14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości e-mail oraz czynności na plikach.
19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
20. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
22. Dashboardsy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
23. Serwer administracyjny musi posiadać możliwość połączenia z serwerem SMTP udostępnianym przez producenta.



Cyberbezpieczny Samorząd

24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.
25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
26. Administrator musi mieć możliwość tworzenia kategorii danych dla plików zaszyfrowanych lub dla takich gdzie zawartość pliku jest niemożliwa do odczytania.
27. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.
28. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, numer REGON, NIP, wyrażenia regularne, określone ciągi znaków i numer IBAN.
29. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
30. Administrator musi mieć możliwość wyszukiwania danych wrażliwych w zasobach lokalnych
1. 31 Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
31. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
32. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
33. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysłaną przez użytkowników Microsoft 365.
34. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
35. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach.
36. System musi umożliwiać synchronizacji grup bezpieczeństwa z Active Directory na potrzeby logowania do konsoli zarządzającej.
37. System musi umożliwiać administratorowi nadanie użytkownikowi uprzywilejowanego dostępu, przez co nie będzie obejmowany politykami przez określony czas – 1 godzinę, 6 godzin lub do końca dnia.
38. System musi posiadać możliwość tworzenia polityk dynamicznych, pozwalających na dostosowywanie się akcji (takich jak zapisywanie logu, powiadomienie użytkownika, blokowanie lub blokowanie z możliwością zastąpienia przez użytkownika) w zależności od profilu pracy użytkownika wykonującego daną czynność, gdzie akcja dobierana jest w zależności od wyniku systemu uczenia maszynowego.
39. System musi umożliwiać dostosowanie polityk dynamicznych do dwóch trybów: standardowy oraz łagodny. Możliwość taka musi istnieć per użytkownik.
40. System musi umożliwiać tworzenie raportów na podstawie logów zebranych w układach danych z możliwością dostosowania filtrów, użytkowników oraz zakresu czasu objętych raportowaniem.
41. System musi umożliwiać utworzenie raportu, który będzie zawierał podsumowanie stanu zabezpieczenia danych wraz z rekomendacjami w formie cyklicznej.



Cyberbezpieczny Samorząd

42. System musi zbierać informacje na temat podłączanych urządzeń do komputera, odwiedzanych domen internetowych, ścieżek sieciowych, drukarek lokalnych oraz sieciowych, umożliwiając jednocześnie przypisanie takowych wpisów do bezpiecznych lub niezaufanych lokalizacji bez potrzeby manualnego wpisywania ścieżek lub numerów seryjnych urządzeń.
43. Dla każdej z wyżej wymienionych lokalizacji system powinien umożliwiać przypisanie indywidualnej polityki dostępu – np. umożliwiając przesyłanie danych do lokalizacji oznaczonej jako bezpieczna, jednocześnie blokując wysyłkę do lokalizacji oznaczonej jako niezaufana lub nieprzypisana.
44. System musi umożliwiać audyt operacji wykonywanych przez administratora w obszarze konsoli DLP.
45. System musi umożliwiać podłączenie archiwa logów w formacie plików o rozszerzeniu md5.

VI. TERMIN WYKONANIA ZAMÓWIENIA

1. Termin zakończenia przedmiotu umowy ustala się na 50 dni licząc od dnia zawarcia umowy

VII. PROJEKTOWANE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI TEJ UMOWY

1. Część II SWZ stanowi projekt umowy, która zostanie zawarta z wykonawcą, którego oferta zostanie uznana za najkorzystniejszą.
2. Ewentualne zmiany dokonane przez wykonawcę we wzorze umowy nie będą przez zamawiającego uwzględnione.
3. Zamawiający przewiduje zmiany umowy. Szczegółowy zakres zmian znajduje się w projekcie umowy w § 9 oraz §9¹.

VIII. 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. Komunikacja między Zamawiającym a Wykonawcami:

- 1) Postępowanie prowadzone jest w języku polskim za pośrednictwem platformazakupowa.pl pod adresem: <https://platformazakupowa.pl/transakcja/1179915>
- 2) W celu skrócenia czasu udzielenia odpowiedzi na pytania komunikacja między zamawiającym a wykonawcami w zakresie:
 - przesyłania Zamawiającemu pytań do treści SWZ;
 - przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia podmiotowych środków dowodowych;
 - przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia/poprawienia/uzupełnienia oświadczenia, o którym mowa w art. 125 ust. 1, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu;
 - przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia wyjaśnień dotyczących treści oświadczenia, o którym mowa w art. 125 ust. 1 lub złożonych podmiotowych środków dowodowych lub innych dokumentów lub oświadczeń składanych w postępowaniu;
 - przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia wyjaśnień dot. treści przedmiotowych środków dowodowych;



Cyberbezpieczny Samorząd

- przestania odpowiedzi na inne wezwania Zamawiającego wynikające z ustawy - Prawo zamówień publicznych;

- przesyłania wniosków, informacji, oświadczeń Wykonawcy;

- przesyłania odwołania/inne

odbywa się za pośrednictwem platformazakupowa.pl i formularza „Wyślij wiadomość do zamawiającego”.

Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przestania za pośrednictwem platformazakupowa.pl poprzez kliknięcie przycisku „Wyślij wiadomość do zamawiającego” po których pojawi się komunikat, że wiadomość została wysłana do zamawiającego.

- 3) Zamawiający będzie przekazywał wykonawcom informacje za pośrednictwem platformazakupowa.pl. Informacje dotyczące odpowiedzi na pytania, zmiany specyfikacji, zmiany terminu składania i otwarcia ofert Zamawiający będzie zamieszczał na platformie w sekcji „Komunikaty”. Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny wykonawca, będzie przekazywana za pośrednictwem platformazakupowa.pl do konkretnego wykonawcy.
- 4) Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na platformazakupowa.pl przesłanych przez zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.
- 5) Zamawiający, zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 30 grudnia 2020r. 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 (Dz. U. z 2020r. poz. 2452), określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na platformazakupowa.pl, tj.:
 - a) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
 - b) komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje,
 - c) zainstalowana dowolna, inna przeglądarka internetowa niż Internet Explorer,
 - d) włączona obsługa JavaScript,
 - e) zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,
 - f) Szyfrowanie na platformazakupowa.pl odbywa się za pomocą protokołu TLS 1.3.
 - g) Oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.
- 6) Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:
 - a) akceptuje warunki korzystania z platformazakupowa.pl określone w Regulaminie zamieszczonym na stronie internetowej [pod linkiem](#) w zakładce „Regulamin” oraz uznaje go za wiążący,
 - b) zapoznał i stosuje się do Instrukcji składania ofert/wniosków dostępnej [pod linkiem](#).
- 7) **Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania z platformazakupowa.pl**, w szczególności za sytuację, gdy zamawiający zapozna się z treścią oferty przed upływem terminu składania ofert (np. złożenie oferty w zakładce „Wyślij wiadomość do zamawiającego”). Taka oferta zostanie uznana przez Zamawiającego za ofertę handlową i nie będzie brana pod uwagę w przedmiotowym



Cyberbezpieczny Samorząd

postępowaniu ponieważ nie został spełniony obowiązek narzucony w art. 221 Ustawy Prawo Zamówień Publicznych.

- 8) Zamawiający informuje, że instrukcje korzystania z platformazakupowa.pl dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu platformazakupowa.pl znajdują się w zakładce „Instrukcje dla Wykonawców” na stronie internetowej pod adresem: <https://platformazakupowa.pl/strona/45-instrukcje>

2. Zalecenia

- 1) Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .xls .jpg (.jpeg) **ze szczególnym wskazaniem na .pdf**
- 2) W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z formatów:
 - a) .zip
 - b) .7Z
- 3) Wśród formatów powszechnych a **NIE występujących** w rozporządzeniu występują: .rar .gif .bmp .numbers .pages. **Dokumenty złożone w takich plikach zostaną uznane za złożone nieskutecznie.**
- 4) Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi max 10MB, oraz na ograniczenie wielkości plików podpisywanych w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi max 5MB.
- 5) Ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu, zamawiający zaleca, w miarę możliwości, przekonwertowanie plików składających się na ofertę na format .pdf i opatrzenie ich podpisem kwalifikowanym PAdES.
- 6) Pliki w innych formatach niż PDF zaleca się opatrzyć zewnętrznym podpisem XAdES. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.
- 7) Zamawiający zaleca, aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju. Podpisywanie różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików.
- 8) Zamawiający zaleca, aby Wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.
- 9) Zaleca się, aby komunikacja z wykonawcami odbywała się tylko na Platformie za pośrednictwem formularza “Wyślij wiadomość do zamawiającego”, nie za pośrednictwem adresu email.
- 10) Osobą składającą ofertę powinna być osoba kontaktowa podawana w dokumentacji.
- 11) Ofertę należy przygotować z należytą starannością dla podmiotu ubiegającego się o udzielenie zamówienia publicznego i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert/wniosków. Sugerujemy złożenie oferty na 24 godziny przed terminem składania ofert/wniosków.
- 12) Podczas podpisywania plików zaleca się stosowanie algorytmu skrótu SHA2 zamiast SHA1.
- 13) Jeśli wykonawca pakuje dokumenty np. w plik ZIP zalecamy wcześniejsze podpisanie każdego ze skompresowanych plików.
- 14) Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.
- 15) Zamawiający zaleca, aby nie wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich podpisem kwalifikowanym. Może to skutkować naruszeniem integralności plików co równoważne będzie z koniecznością odrzucenia oferty w postępowaniu.



Cyberbezpieczny Samorząd

IX. INFORMACJE O SPOSOBIE KOMUNIKOWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI W INNY SPOSÓB NIŻ PRZY UŻYCIU ŚRODKÓW KOMUNIKACJI ELEKTRONICZNEJ W PRZYPADKU ZAISTNIENIA JEDNEJ Z SYTUACJI OKREŚLONYCH W ART. 65 UST. 1, ART. 66 I ART. 69

Nie dotyczy.

X. WSKAZANIE OSÓB UPRAWNIONYCH DO KOMUNIKOWANIA SIĘ Z WYKONAWCAMI

1. Osobą uprawnioną do komunikowania się z wykonawcami jest:
 - 1) w zakresie proceduralnym: **Bartosz Bielecki**, e-mail: przetargi@golancz.pl
 - 2) w zakresie merytorycznym: **Mateusz Gawkowski**, e-mail: informatyk@golancz.pl,
2. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ.
3. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert.
4. Jeżeli zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w ust. 3, przedłuża termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia ofert.
5. W przypadku, gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie, o którym mowa w ust. 3, zamawiający nie ma obowiązku udzielania wyjaśnień SWZ oraz obowiązku przedłużenia terminu składania ofert.
6. Przedłużenie terminu składania ofert, nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.
7. W przypadku rozbieżności pomiędzy treścią SWZ, a treścią udzielonych odpowiedzi jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.

XI. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca jest związany ofertą do dnia **01 listopada 2025 roku**. Bieg terminu związania ofertą rozpoczyna się w dniu, w którym upływa termin składania ofert.
2. Szczegółowe informacje dotyczące terminu związania ofertą określono w przepisach m.in. art. 220 ustawy P.z.p.

XII. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

1. Wykonawca może złożyć tylko jedną ofertę.
2. Ofertę wraz z wymaganymi dokumentami należy umieścić na platformazakupowa.pl pod adresem: <https://platformazakupowa.pl/transakcja/1179915> w myśl Ustawy na stronie internetowej prowadzonego postępowania.
3. Do oferty należy dołączyć wszystkie wymagane w SWZ dokumenty.
4. Po wypełnieniu Formularza składania oferty lub wniosku i dołączenia wszystkich wymaganych załączników należy kliknąć przycisk „Przejdź do podsumowania”.
5. Oferta lub wniosek 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



Cyberbezpieczny Samorząd

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.

6. 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.
7. Szczegółowa instrukcja dla Wykonawców dotycząca złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem: <https://platformazakupowa.pl/strona/45-instrukcje>
8. Oferta zostanie sporządzona na **Formularzu ofertowym** stanowiącym **załącznik nr 1** do SWZ. Wraz z ofertą wykonawca jest zobowiązany złożyć dokumenty wskazane **w Rozdziale XXI**. Treść oferty musi być zgodna z wymaganiami zamawiającego określonymi w dokumentach zamówienia.
9. Oferta może być złożona tylko do upływu terminu składania ofert. Do upływu terminu składania ofert wykonawca może wycofać ofertę.
10. Oferta oraz pozostałe oświadczenia i dokumenty, dla których zamawiający określił wzory w formie formularzy zamieszczonych w załącznikach do SWZ, powinny być sporządzone zgodnie z tymi wzorami, co do treści oraz opisu kolumn i wierszy.
11. Ofertę sporządza się w języku polskim. Podmiotowe środki dowodowe, przedmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski.
12. W przypadku, gdy podmiotowe środki dowodowe, inne dokumenty lub dokumenty potwierdzające umocowanie do reprezentowania odpowiednio wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, podmiotu udostępniającego zasoby na zasadach określonych w art. 118 ustawy P.z.p. lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach, zostały wystawione przez upoważnione podmioty inne niż wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, jako dokument elektroniczny, przekazuje się ten dokument.
13. Upoważnienie do podpisania oferty winno być dołączone do oferty, o ile nie wynika to z innych dokumentów załączonych do oferty (np. z odpisu z rejestru sądowego, zaświadczenia o wpisie do CEIDG).
14. Wszystkie formularze zawarte w niniejszej SWZ, a w szczególności Formularz oferty – wykonawca wypełni ściśle według wskazówek zawartych w SWZ. W przypadku, gdy jakkolwiek część dokumentów nie dotyczy wykonawcy – wypełnia „nie dotyczy”.
15. Postępowanie o udzielenie zamówienia jest jawne. Nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913), zwaną dalej ustawą z.n.k, jeżeli wykonawca, wraz z przekazaniem takich informacji, zastrzegł, że nie mogą być one udostępniane oraz wykazał, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w Rozdziale XIV ust. 4 SWZ.
16. W przypadku, gdy dokumenty elektroniczne w postępowaniu przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z.n.k, wykonawca, w celu utrzymania w poufności tych informacji, **przekazuje je w wydzielonym i odpowiednio oznaczonym pliku:**
 - 1) Wykonawca załączając plik oznacza czy jest on jawny oraz czy zawiera dane osobowe;



Cyberbezpieczny Samorząd

- 2) W przypadku oznaczenia pliku jako niejawnego wykonawca zobowiązany jest wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
17. Przez tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z.n.k rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności.
18. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.

XIII. SPOSÓB ORAZ TERMIN SKŁADANIA OFERT

1. Ofertę składa się pod rygorem nieważności w formie elektronicznej (opatrzonej kwalifikowanym podpisem elektronicznym).
2. Ofertę należy złożyć poprzez Platformę Zamówień Publicznych platformazakupowa.pl: pod adresem <https://platformazakupowa.pl/transakcja/1179915> do dnia 03 października 2025 r. do godziny 10:00.
3. Za datę przekazania oferty przyjmuje się datę jej przekazania do Systemu.

XIV. TERMIN OTWARCIA OFERT

1. Otwarcie ofert następuje w dniu 03 października września 2025 roku o godzinie 10:05.
2. Otwarcie ofert następuje niezwłocznie po upływie terminu składania ofert, nie później niż następnego dnia po dniu, w którym upłynął termin składania ofert.
3. Zamawiający najpóźniej przed otwarciem ofert, udostępnia się na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza się przeznaczyć na sfinansowanie zamówienia.
4. Jeżeli otwarcie ofert następuje przy użyciu systemu teleinformatycznego, w przypadku awarii tego systemu, która powoduje brak możliwości otwarcia ofert w terminie określonym przez zamawiającego, otwarcie ofert następuje niezwłocznie po usunięciu awarii.
5. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
6. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informację 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”.



XV. PODSTAWY WYKLUCZENIA Z POSTĘPOWANIA

1. Z postępowania o udzielenie zamówienia wyklucza się wykonawców, w stosunku do których zachodzi którakolwiek z okoliczności wskazanych:
 - 1) w art. 108 ust. 1 ustawy P.z.p;
 - 2) w art. 109 ust. 1 pkt 4 ustawy P.z.p., tj.:

w stosunku, do którego otwarto likwidację, ogłoszono upadłość, którego aktywami 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.
2. Wykluczenie wykonawcy następuje zgodnie z art. 111 ustawy P.z.p. (odnośnie podstaw, których dotyczy).
3. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2 i 5 lub art. 109 ust. 1 pkt. 4, jeżeli udowodni zamawiającemu, że spełnił łącznie następujące przesłanki:
 - 1) naprawił lub zobowiązał się do naprawienia szkody wyrządzonej przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem, w tym poprzez zadośćuczynienie pieniężne;
 - 2) wyczerpująco wyjaśnił fakty i okoliczności związane z przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem oraz spowodowanymi przez nie szkodami, aktywnie współpracując odpowiednio z właściwymi organami, w tym organami ścigania, lub zamawiającym;
 - 3) podjął konkretne środki techniczne, organizacyjne i kadrowe, odpowiednie dla zapobiegania dalszym przestępstwom, wykroczeniom lub nieprawidłowemu postępowaniu, w szczególności:
 - a) zerwał wszelkie powiązania z osobami lub podmiotami odpowiedzialnymi za nieprawidłowe postępowanie wykonawcy,
 - b) zreorganizował personel,
 - c) wdrożył system sprawozdawczości i kontroli,
 - d) utworzył struktury audytu wewnętrznego do monitorowania przestrzegania przepisów, wewnętrznych regulacji lub standardów,
 - e) wprowadził wewnętrzne regulacje dotyczące odpowiedzialności i odszkodowań za nieprzestrzeganie przepisów, wewnętrznych regulacji lub standardów.
4. Zamawiający ocenia, czy podjęte przez wykonawcę czynności, o których mowa w pkt. 3, są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu wykonawcy. Jeżeli podjęte przez wykonawcę czynności, o których mowa w pkt. 3, nie są wystarczające do wykazania jego rzetelności, zamawiający wyklucza wykonawcę.



XVa PODSTAWY WYKLUCZENIA NA PODSTAWIE USTAWY Z DNIA 7 KWIETNIA 2022 R. O SZCZEGÓLNYCH ROZWIĄZANIACH W ZAKRESIE PRZECIWDZIAŁANIA WSPIERANIU AGRESJI NA UKRAINĘ ORAZ SŁUŻĄCYCH OCHRONIE BEZPIECZEŃSTWA NARODOWEGO

1. Na podstawie ustawy z dnia 7 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (tj. Dz. U. z 2025 r. poz. 514) (zwanej dalej „ustawą s.r.p.w.a.n.u”) z postępowania o udzielenie zamówienia publicznego wyklucza się:
 - 1) wykonawcę 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 s.r.p.w.a.n.u (wykluczenie z postępowania);
 - 2) wykonawcę, 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 s.r.p.w.a.n.u (wykluczenie z postępowania);
 - 3) wykonawcę, 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 s.r.p.w.a.n.u (wykluczenie z postępowania).
2. Wykluczenie następuje na okres trwania okoliczności określonych w ust. 1.
3. W przypadku wykonawcy wykluczonego na podstawie ust. 1, zamawiający odrzuca ofertę takiego wykonawcy na podstawie art. 226 ust. 1 pkt 2 lit. a ustawy Pzp w związku z art. 7 ust. 3 ustawy s.r.p.w.a.n.u.¹
4. Kontrola udzielania zamówień publicznych w zakresie zgodności z ust. 1 jest wykonywana zgodnie z art. 596 ustawy pzp.
5. Przez ubieganie się o udzielenie zamówienia publicznego rozumie się złożenie oferty.²
6. Osoba lub podmiot podlegające wykluczeniu na podstawie ust. 1, które w okresie tego wykluczenia ubiegają się o udzielenie zamówienia publicznego lub biorą udział w postępowaniu o udzielenie zamówienia publicznego, podlegają karze pieniężnej.
7. Karę pieniężną, o której mowa w ust. 6, nakłada Prezes Urzędu Zamówień Publicznych w drodze decyzji, do wysokości 20 000 000 zł.

¹ odrzuca wniosek o dopuszczenie do udziału w postępowaniu lub ofertę takiego wykonawcy, nie zaprasza go do złożenia oferty wstępnej, oferty podlegającej negocjacom, oferty dodatkowej, oferty lub oferty ostatecznej, nie zaprasza go do negocjacji lub dialogu, a także nie prowadzi z takim wykonawcą negocjacji lub dialogu, odpowiednio do trybu stosowanego do udzielenia zamówienia oraz etapu prowadzonego postępowania;

² odpowiednio złożenie wniosku o dopuszczenie do udziału w postępowaniu, złożenie oferty, przystąpienie do negocjacji;



8. W zakresie nieuregulowanym w ust. 6 i 7 do nakładania i wymierzania kary pieniężnej, o której mowa w ust. 6, stosuje się przepisy działu IVa ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego.
9. Wpływy z kar pieniężnych, o których mowa w ust. 6, stanowią dochód budżetu państwa.

UWAGA!!!: w celu wykazania braku podstaw wykluczenia z ww. podstawy prawnej Wykonawca jest zobowiązany do złożenia oświadczenia o braku podstaw wykluczenia w ww. zakresie na załączniku nr 2a.

Załącznik nr 2a do SWZ składa Wykonawca oraz każdy z wykonawców wspólnie ubiegających się o zamówienie, podmiot/-ty udostępniający/-ce swoje zasoby

XVI. SPOSÓB OBLICZENIA CENY

1. Cenę oferty dla każdej części należy obliczyć jako iloczyn podanej ilości sprzętu wskazanych przez Zamawiającego w SWZ oraz podanych przez Wykonawcę cen jednostkowych. Cena musi zawierać wszystkie koszty związane z realizacją zamówienia wraz z podatkiem VAT obowiązującym w dacie sporządzenia oferty. Stawka podatku VAT musi zostać określona zgodnie z ustawą z dn. 11.03.2004 r. o podatku od towarów i usług (tj. Dz. U. z 2025 r. poz. 775 z późn. zm.).
2. Wykonawca określi cenę oferty składając ofertę na realizację przedmiotu zamówienia w załączniku nr 1 do SWZ. Cena podana na Formularzu Ofertowym jest ceną ryczałtową, ostateczną, niepodlegającą negocjacji i wyczerpującą wszelkie należności Wykonawcy wobec Zamawiającego związane z realizacją przedmiotu zamówienia.
3. Cenę oferty należy podać do dwóch miejsc po przecinku.
4. Zaoferowana cena musi uwzględniać wykonanie zamówienia zgodnie z postanowieniami SWZ i jej załącznikami, w szczególności:
 1. ceny jednostkowe sprzętu wskazanego w opisie przedmiotu zamówienia w SWZ;
 2. koszty dostawy do wskazanych w SWZ przez Zamawiającego punktów dostawy.
 3. Inne koszty niezbędne do prawidłowej realizacji zamówienia.
5. Jeżeli zaoferowana cena lub jej istotne części składowe, wydają się rażąco niskie w stosunku do przedmiotu zamówienia lub budzą wątpliwości zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi w dokumentach zamówienia lub wynikającymi z odrębnych przepisów, zamawiający żąda od wykonawcy **wyjaśnień, w tym** złożenia dowodów w zakresie wyliczenia ceny, lub jej istotnych części składowych.
6. **W przypadku gdy cena całkowita oferty złożonej w terminie jest niższa o co najmniej 30% od:**
 - 1) wartości zamówienia powiększonej o należny podatek od towarów i usług, ustalonej przed wszczęciem postępowania lub średniej arytmetycznej cen wszystkich złożonych ofert niepodlegających odrzuceniu na podstawie art. 226 ust. 1 pkt 1 i 10, zamawiający zwraca się o udzielenie wyjaśnień, o których mowa w pkt. 5, chyba że rozbieżność wynika z okoliczności oczywistych, które nie wymagają wyjaśnienia;
 - 2) wartości zamówienia powiększonej o należny podatek od towarów i usług, zaktualizowanej z uwzględnieniem okoliczności, które nastąpiły po wszczęciu



postępowania, w szczególności istotnej zmiany cen rynkowych, zamawiający może zwrócić się o udzielenie wyjaśnień, o których mowa w pkt. 5.

7. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu spoczywa na Wykonawcy.
8. Odrzuceniu jako oferta z rażąco niską ceną lub kosztem, podlega oferta wykonawcy, który nie udzielił wyjaśnień w wyznaczonym terminie, lub jeżeli złożone wyjaśnienia wraz z dowodami nie uzasadniają podanej w ofercie ceny.
9. Jeżeli została złożona oferta, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z ustawą o podatku od towarów i usług, dla celów zastosowania kryterium ceny zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć.
10. Wzór Formularza Ofertowego został opracowany przy założeniu, że wybór oferty nie będzie prowadzić do powstania u zamawiającego obowiązku podatkowego w zakresie podatku VAT. W przypadku, gdy wybór oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego w zakresie podatku VAT wykonawca zobowiązany jest złożyć oświadczenie o powstaniu u zamawiającego obowiązku podatkowego, odpowiednio modyfikując treść Formularza Ofertowego poprzez wprowadzenie w Informacjach dodatkowych odpowiednich postanowień tj. w ofercie, o której mowa w pkt. 9, wykonawca ma obowiązek:
 - 1) poinformowania zamawiającego, że wybór jego oferty będzie prowadził do powstania u zamawiającego obowiązku podatkowego;
 - 2) wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;
 - 3) wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku;
 - 4) wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie.

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

1. Przy wyborze najkorzystniejszej oferty zamawiający będzie się kierował kryterium:

Nazwa	Opis	Znaczenie (waga)w %
Cena (C)	Cena brutto oferty obliczona zgodnie z rozdziałem XVI	100

2. **Opis sposobu oceny ofert.**

Ocenie ofert będą podlegały tylko oferty niepodlegające odrzuceniu.

Każda oferta zostanie oceniona w następujący sposób:

- 1) W pierwszej kolejności zostanie obliczona liczba punktów osobno dla każdego kryterium wg poniższych wzorów:
 - a) Liczba punktów w kryterium „Cena)(C) zostanie obliczona wg wzoru:

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



gdzie:

C_{min} – cena brutto oferty najtańszej

C_o – cena brutto oferty ocenianej

3. **Za najkorzystniejszą zostanie uznana oferta, która uzyska największą ilość punktów.**
4. **W toku badania i oceny ofert zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych ofert lub innych składanych dokumentów lub oświadczeń.**
5. **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.
6. W przypadku, o którym mowa w ust. 5 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.

XVIII. INFORMACJA 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 w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty.
2. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 1, jeżeli w postępowaniu o udzielenie zamówienia prowadzonym w trybie podstawowym złożono tylko jedną ofertę.
3. 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 oraz wybrać najkorzystniejszą ofertę albo unieważnić postępowanie.
4. Wykonawca będzie zobowiązany do podpisania umowy w miejscu i terminie wskazanym przez zamawiającego.
5. UWAGA! – Umowa zawierana jest pod rygorem nieważności w formie pisemnej, tym samym Zamawiający dopuszcza możliwość podpisania umowy przy użyciu kwalifikowanego podpisu elektronicznego lub osobiście na miejscu w siedzibie Zamawiającego.

XIX. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

1. Środki ochrony prawnej określone w Dziale IX ustawy P.z.p. przysługują wykonawcom oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy P.z.p.



Cyberbezpieczny Samorząd

2. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 ustawy P.z.p. oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
3. Wniesienie odwołania następuję w terminach i na warunkach określonych w dziale IX ustawy P.z.p.
4. Zaleca się aby odwołanie lub jego kopię, o których mowa w art. 514 ust. 2 ustawy P.z.p., przekazać Zamawiającemu przy użyciu strony internetowej prowadzonego postępowania.

XX. INFORMACJA O WARUNKACH UDZIAŁU W POSTĘPOWANIU

1. **O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy:**
 - 1) nie podlegają wykluczeniu;
 - 2) spełniający warunki udziału w postępowaniu określone w niniejszej SWZ.
2. **Warunki udziału w postępowaniu mogą dotyczyć:**
 - 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.
3. **O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy spełniają warunki dotyczące:**
 - 1) **zdolności do występowania w obrocie gospodarczym:**
Zamawiający nie stawia warunku w powyższym zakresie.
 - 2) **uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:**
Zamawiający nie stawia warunku w powyższym zakresie.
 - 1) **sytuacji ekonomicznej lub finansowej:**
Zamawiający nie stawia warunku w powyższym zakresie.
 - 3) **zdolności technicznej lub zawodowej:**
Zamawiający nie stawia warunku w powyższym zakresie.

XXI. WYKAZ OŚWIADCZEŃ I DOKUMENTÓW SKŁADANYCH WRAZ Z FORMULARZEM OFERTOWYM

1. **Dokumenty składane wraz z Formularzem ofertowym - załącznik nr 1 do SWZ:**
 - 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 dotyczące podstaw wykluczenia 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 - oświadczenie składane **na załączniku nr 2a do SWZ**;
 - 3) W celu potwierdzenia, że osoba działająca w imieniu wykonawcy jest umocowana do jego reprezentowania, zamawiający żąda od wykonawcy odpisu lub informacji 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 powyżej, 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 powyżej, zamawiający może żądać od wykonawcy pełnomocnictwa lub innego dokumentu potwierdzającego umocowanie do reprezentowania wykonawcy. Przepis stosuje się odpowiednio do osoby działającej w imieniu wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego oraz osoby działającej w imieniu podmiotu udostępniającego zasoby na zasadach określonych w art. 118 ustawy P.z.p.

- 4) **Pełnomocnictwo lub inny dokument potwierdzający umocowanie do reprezentowania wykonawcy należy przedłożyć** w formie elektronicznej (podpisane kwalifikowanym podpisem elektronicznym), lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym. Pełnomocnictwo musi być wystawione w sposób określony przepisami prawa cywilnego.
- 5) Osoba lub osoby składające ofertę ponoszą pełną odpowiedzialność za treść złożonego oświadczenia woli na zasadach określonych w art. 297 § 1 Kodeksu karnego (Dz. U. z 2020 r. poz. 1444 z późn. zm.).

XXII. INFORMACJA O PODMIOTOWYCH ŚRODKACH DOWODOWYCH - OŚWIADCZENIA I DOKUMENTY, JAKIE ZOBOWIĄZANI SĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ WYKAZANIA BRAKU PODSTAW WYKLUCZENIA

1. Do oferty wykonawca zobowiązany jest dołączyć aktualne na dzień składania ofert oświadczenie o braku podstaw do wykluczenia – zgodnie z **Załącznikiem nr 2 i 2a do SWZ**.
2. W przypadku **wspólnego ubiegania się o zamówienie przez wykonawców**, oświadczenie, o którym mowa w ust. 1, **składa każdy z wykonawców**. Oświadczenia te potwierdzają brak podstaw wykluczenia każdego z wykonawców.
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, aktualnych na dzień złożenia podmiotowych środków dowodowych:
 - 1) Oświadczenia wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy P.z.p., o braku przynależności 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 późn. zm.), z innym wykonawcą, który złożył odrębną ofertę, ofertę częściową albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej – **załącznik nr 3 do SWZ**;
 - 2) Odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy P.z.p., sporządzonych nie wcześniej **niż 3 miesiące** przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji.
4. Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast odpisu albo informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, o których mowa w ust. 3 pkt 2 - składa dokument lub



Cyberbezpieczny Samorząd

dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające, że:

- 1) nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury.
5. Dokument, o którym mowa w ust. 4 pkt 1, powinien być wystawiony nie wcześniej niż 3 miesiące przed ich złożeniem.
6. Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w ust. 4, 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. Dokument, powinien być wystawiony nie wcześniej niż 3 miesiące przed jego złożeniem.
7. 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 (zgodnie z **Załącznikiem nr 2 do SWZ**), dane umożliwiające dostęp do tych środków w oparciu o art. 274 ust. 4 ustawy P.z.p.).
8. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które zamawiający posiada, jeżeli wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.
9. Zamawiający może żądać od wykonawców wyjaśnień dotyczących treści oświadczenia, o którym mowa w art. 125 ust. 1 ustawy P.z.p., lub złożonych podmiotowych środków dowodowych lub innych dokumentów lub oświadczeń składanych w postępowaniu.
10. W zakresie nieuregulowanym SWZ, zastosowanie mają 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 (Dz. U. 2020 poz. 2415).

XXIII. 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.
2. W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenia, o których mowa w Rozdziale XXII ust. 1 SWZ, składa każdy z wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia.
3. W przypadku, gdy oferta wykonawcy wspólnie ubiegającego zostanie najwyższej oceniona, każdy z wykonawców składa dokumenty, o których mowa w Rozdziale XXII ust. 3 SWZ.
4. Oświadczenia i dokumenty potwierdzające brak podstaw do wykluczenia z postępowania składa każdy z wykonawców wspólnie ubiegających się o zamówienie.



5. W przypadku wyboru oferty złożonej przez wykonawców wspólnie ubiegających się o udzielenie zamówienia zamawiający zastrzega sobie prawo żądania przed zawarciem umowy w sprawie zamówienia publicznego umowy regulującej współpracę tych wykonawców.

XXIV. OPIS CZĘŚCI ZAMÓWIENIA

Oferta musi obejmować całość zamówienia, nie dopuszcza się składania ofert częściowych. Zamawiający odstąpił od podziału zamówienia na części z uwagi na obawę, że podział taki przełożyłby się na nadmierne trudności techniczne, oraz nadmierne koszty wykonania zamówienia, a także potrzebę skoordynowania wielu działań, co mogłoby poważnie zagrozić właściwemu wykonaniu zamówienia. Wskazane powody Zamawiający ustalił po uwzględnieniu całokształtu okoliczności związanych z przedmiotem zamówienia.

XXV. LICZBA CZĘŚCI ZAMÓWIENIA, NA KTÓRĄ WYKONAWCA MOŻE ZŁOŻYĆ OFERTĘ, MAKSYMALNA LICZBA CZĘŚCI, NA KTÓRE ZAMÓWIENIE MOŻE ZOSTAĆ UDZIELONE TEMU SAMEMU WYKONAWCY, ORAZ KRYTERIA /ZASADY, MAJĄCE ZASTOSOWANIE DO USTALENIA, KTÓRE CZĘŚCI ZAMÓWIENIA ZOSTANĄ UDZIELONE JEDNEMU WYKONAWCY, W PRZYPADKU WYBORU JEGO OFERTY W WIĘKSZEJ NIŻ MAKSYMALNA LICZBIE CZĘŚCI

Nie dotyczy.

XXVI. INFORMACJA DOTYCZĄCA OFERT WARIANTOWYCH, W TYM INFORMACJA O SPOSOBIE PRZEDSTAWIANIA OFERT WARIANTOWYCH ORAZ MINIMALNE WARUNKI, JAKIM MUSZĄ ODPOWIEDZIEĆ OFERTY WARIANTOWE

Zamawiający nie dopuszcza możliwości złożenia oferty wariantowej przewidującej odmienny niż określony w SWZ sposób wykonania zamówienia.

XXVII. WYMAGANIA W ZAKRESIE ZATRUDNIENIA NA PODSTAWIE STOSUNKU PRACY, W OKOLICZNOŚCIACH, O KTÓRYCH MOWA W ART. 95

Nie dotyczy.

XXVIII. WYMAGANIA W ZAKRESIE ZATRUDNIENIA OSÓB, O KTÓRYCH MOWA W ART. 96 UST. 2 PKT 2

Zamawiający nie przewiduje zatrudnienia w zakresie określonym w art. 96 ust. 2 pkt 2 ustawy P.z.p.

XXIX. INFORMACJA O ZASTRZEŻENIU MOŻLIWOŚCI UBIEGANIA SIĘ O UDZIELENIE ZAMÓWIENIA WYŁĄCZNIE PRZEZ WYKONAWCÓW, O KTÓRYCH MOWA W ART. 94

Zamawiający nie zastrzega możliwości ubiegania się o udzielenie zamówienia wyłącznie przez wykonawców, o których mowa w art. 94 ustawy P.z.p.



XXX. WYMAGANIA DOTYCZĄCE WADIUM, W TYM JEGO KWOTA

Oferent nie wnosi wadium.

XXXI. INFORMACJA O PRZEWIDYWANYCH ZAMÓWIENIACH, O KTÓRYCH MOWA W ART. 214 UST. 1 PKT 7 I 8

Zamawiający nie przewiduje udzielenia zamówień, o których mowa w art. 214 ust. 1 pkt 8 ustawy Pzp.

XXXII. INFORMACJA DOTYCZĄCA PRZEPROWADZENIA PRZEZ WYKONAWCĘ WIZJI LOKALNEJ LUB SPRAWDZENIA PRZEZ NIEGO DOKUMENTÓW NIEZBĘDNYCH DO REALIZACJI ZAMÓWIENIA, O KTÓRYCH MOWA W ART. 131 UST. 2

Zamawiający nie wymaga przeprowadzenia przez wykonawcę wizji lokalnej lub sprawdzenia przez niego dokumentów niezbędnych do realizacji zamówienia, o których mowa w art. 131 ust. 2 ustawy P.z.p.

XXXIII. INFORMACJA DOTYCZĄCA WALUT OBCYCH, W JAKICH MOGĄ BYĆ PROWADZONE ROZLICZENIA MIĘDZY ZAMAWIAJĄCYM A WYKONAWCĄ

1. Rozliczenia między zamawiającym a wykonawcą prowadzone będą wyłącznie w polskiej walucie.
2. Jeżeli wykonawca przedstawi dokumenty, w których wartość podana będzie w innej walucie niż PLN, to dla potwierdzenia spełnienia warunków zamawiający dokona przeliczenia tej waluty na PLN według średniego bieżącego kursu wyliczonego i ogłoszonego przez Narodowy Bank Polski z dnia wszczęcia postępowania o udzielenie zamówienia publicznego (za datę wszczęcia postępowania zamawiający uznaje datę publikacji ogłoszenia o zamówieniu w DUUE, zamieszczenia ogłoszenia o zamówieniu w miejscu publicznie dostępnym w swojej siedzibie oraz na stronie internetowej). Kursy walut dostępne są pod następującym adresem internetowym: <http://www.nbp.pl> Jeżeli w tym dniu nie będzie opublikowany średni kurs NBP, zamawiający przyjmie kurs średni z ostatniej tabeli przed dniem wszczęcia postępowania.

XXXIV. INFORMACJA DOTYCZĄCA ZWROTU KOSZTÓW UDZIAŁU W POSTĘPOWANIU

Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

XXXV. INFORMACJA O OBOWIĄZKU OSOBISTEGO WYKONANIA PRZEZ WYKONAWCĘ KLUCZOWYCH ZADAŃ ZGODNIE Z ART. 60 I ART. 121

1. Zamawiający nie przewiduje obowiązku osobistego wykonania przez wykonawcę kluczowych zadań zgodnie z art. 60 ustawy P.z.p. i art. 121 ustawy P.z.p.
2. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy (podwykonawcom).



3. Zamawiający wymaga, aby w przypadku powierzenia części zamówienia podwykonawcom, wykonawca wskazał w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom oraz podał nazwy ewentualnych podwykonawców, jeżeli są znani.

XXXVI. MAKSYMALNA LICZBA WYKONAWCÓW, Z KTÓRYMI ZAMAWIAJĄCY ZAWRZE UMOWĘ RAMOWĄ

Zamawiający nie przewiduje zawierania umowy ramowej.

XXXVII. INFORMACJA O PRZEWIDYWANYM WYBORZE NAJKORZYSTNIEJSZEJ OFERTY Z ZASTOSOWANIEM AUKCJI ELEKTRONICZNEJ WRAZ Z INFORMACJAMI, O KTÓRYCH MOWA W ART. 230

Zamawiający nie przewiduje zastosowania aukcji elektronicznej.

XXXVIII. WYMÓG LUB MOŻLIWOŚĆ ZŁOŻENIA OFERT W POSTACI KATALOGÓW ELEKTRONICZNYCH LUB DOŁĄCZENIA KATALOGÓW ELEKTRONICZNYCH DO OFERTY, W SYTUACJI OKREŚLONEJ W ART. 93

Zamawiający nie przewiduje złożenia ofert w postaci katalogów elektronicznych lub dołączenia katalogów elektronicznych do oferty, w sytuacji określonej w art. 93 ustawy p.z.p.

XXXIX. INFORMACJA DOTYCZĄCA ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

XL. OBOWIĄZEK INFORMACYJNY WYNIKAJĄCY Z ART. 13 RODO W PRZYPADKU ZBIERANIA DANYCH OSOBOWYCH BEZPOŚREDNIO OD OSOBY FIZYCZNEJ, KTÓREJ DANE DOTYCZĄ, W CELU ZWIĄZANYM Z POSTĘPOWANIEM O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO

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).

Informuję, że:

1. Administratorem Pani/Pana danych osobowych jest Miasto i Gmina Gołańcz. Siedzibą Administratora Danych jest: 62-130 Gołańcz, ul. Dr P. Kowalika 2, tel.: +48 (67)2615911, fax.: +48 (67)2683312, e-mail: miastoigmina@golancz.pl
2. Administrator Danych powołał Inspektora Ochrony Danych. Kontakt z IOD możliwy jest poprzez: kontakt osobisty w siedzibie Urzędu Miasta i Gminy Gołańcz, ul. Dr P. Kowalika 2, 62-130 Gołańcz – pok. nr 12, adres e-mail: inspektor@cbi24.pl
3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego (szczegółowy zakres, tryb postępowania, nazwa i numer zadania znajduje się w Specyfikacji Warunków Zamówienia).



Cyberbezpieczny Samorząd

4. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 94 ust. 1 ustawy z dnia 11 września 2019r. Prawo Zamówień Publicznych (*Dz. U. z 2019 r. poz. 2019 z późn. zm.*), zwaną dalej ustawą P.z.p..
5. Dane osobowe będą przechowywane zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji zakresu działania archiwów zakładowych (*Dz. U. Nr 14, poz. 67 z późn. zm.*) oraz rozporządzeniem Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej (*Dz. U. z 2019 r. poz. 246*). W przypadku zamówień publicznych finansowanych ze źródeł zewnętrznych okres przechowywania i postępowania z dokumentacją szczegółowo określają umowy.
6. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy P.z.p., związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy P.z.p..
7. W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO.
8. Posiada Pani/Pan:
 - 1) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
 - 2) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych *;
 - 3) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO **;
 - 4) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

* Wyjaśnienie: skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą P.z.p. oraz nie może naruszać integralności protokołu oraz jego załączników.

** Wyjaśnienie: 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.

9. Nie przysługuje Pani/Panu:
 - 1) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
 - 2) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
 - 3) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

ZAŁĄCZNIKI DO CZĘŚCI I – SWZ - INTEGRALNĄ CZĘŚĆ NINIEJSZEJ SWZ STANOWIĄ WZORY NASTĘPUJĄCYCH DOKUMENTÓW:

nr 1 – Formularz ofertowy;



Cyberbezpieczny Samorząd

- nr 2 – Oświadczenie o braku podstaw do wykluczenia z postępowania;
- nr 2a - Oświadczenie dotyczące podstaw wykluczenia 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
- nr 3 – Oświadczenie Wykonawcy o braku przynależności do tej samej grupy kapitałowej;
- nr 4 – Projekt umowy;

Załącznik 1 do SWZ

Formularz ofertowy





Cyberbezpieczny Samorząd

Pełna nazwa wykonawcy

Adres siedziby wykonawcy

Kod

Ulica.....

Miasto.....

WojewództwoNr NIP (w przypadku
wykonawców wspólnych uzupełnić dla każdego wykonawcy)

Nr REGON.....(w przypadku wykonawców wspólnych uzupełnić dla każdego
wykonawcy)

Nr konta bankowego

Adres konta wykonawcy w systemie

Nr telefonu

E-mail:

Rodzaj wykonawcy: (wybrać odpowiednie poniżej):*

- ☐ mikroprzedsiębiorstwo
- ☐ małe przedsiębiorstwo
- ☐ średnie przedsiębiorstwo
- ☐ jednoosobowa działalność gospodarcza
- ☐ osoba fizyczna nieprowadząca działalności gospodarczej
- ☐ inny rodzaj

Miasto i Gmina Gołańcz

reprezentowana przez

inż. Roberta Torza – Burmistrza Miasta i Gminy Gołańcz

Adres: ul. Doktora Piotra Kowalika 2, 62 – 130 Gołańcz

OFERTA

Nawiązując do ogłoszenia dotyczącego postępowania na wykonanie usługi: związanych z zadaniem **Cyberbezpieczny Samorząd** Oferujemy wykonanie przedmiotu zamówienia określonego w Specyfikacji Warunków Zamówienia (SWZ), za wynagrodzeniem ryczałtowym.....zł (netto)+.....% podatku VAT, tj. **ogółem zł brutto**

Zestawienie zaoferowanego przedmiotu zamówienia zgodnie z wymaganiami specyfikacji warunków zamówienia:



Cyberbezpieczny Samorząd

Lp.	Nazwa	Cena jednostkowa netto za 1 szt.	Stawka podatku VAT (%)	Cena jednostkowa brutto za 1 szt.	Ilość Sztuk	Wartość brutto (kolumna nr 5 x kolumna nr 6)
1	2	3	4	5	6	7
1.	Serwer wraz z systemem operacyjnym oraz licencjami dostępowymi dla użytkowników				2	
2.	Macierz dyskowa				1	
3.	Przełączniki sieciowe				4	
4.	Rozwiązania zasilania awaryjnego - UPS				1	
5.	System do gromadzenia i analizy zapisów działań w systemach wraz ze wsparciem na czas trwania projektu				1	
6.	System kopii zapasowych				1	
7.	Zakup systemu zabezpieczającego przed wyciekami danych z organizacji				1	
RAZEM WARTOŚĆ OFERTY BRUTTO						

- Oświadczamy, że zapoznaliśmy się ze SWZ i uznajemy się za związanych określonymi w niej wymaganiami i zasadami postępowania.
- Oświadczamy, że uważamy się za związanych niniejszą ofertą na czas wskazany w SWZ.
- Prace objęte zamówieniem zamierzamy wykonać:
 - ☐ sami
 - ☐ siłami podwykonawcy:
 - Część zamówienia, którą wykonywać będzie podwykonawca:
 - nazwa podwykonawcy/ ów
- Oświadczamy, że zawarty w SWZ projekt umowy został przez nas zaakceptowany i zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy na wyżej wymienionych warunkach w miejscu i terminie wyznaczonym przez zamawiającego.
- Oświadczamy, że oferujemy zamawiającemu okres płatności **do 30 dni** od złożonej faktury wystawionej za zrealizowany przedmiot umowy licząc od dnia dostarczenia prawidłowo wystawionej faktury do Zamawiającego.



Cyberbezpieczny Samorząd

6. Oświadczamy, że oferta zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Informacje takie zawarte są w następujących dokumentach:
7. Wykonanie zamówienia będzie/nie będzie³ prowadziło do powstania u Zamawiającego obowiązku podatkowego. W przypadku, kiedy wykonanie zamówienia będzie prowadziło do powstania u Zamawiającego obowiązku podatkowego, Wykonawca musi wskazać nazwę (rodzaj) towaru lub usługi, która będzie prowadziła do jego powstania oraz wskazać jej wartość bez kwoty podatku.
8. Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

UWAGA: 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 ww. oświadczenia wykonawca nie składa - wówczas należy usunąć treść oświadczenia przez jego wykreślenie.

Załącznikami do niniejszej oferty są:

1.
2.
3.

**Wykonawca wskazuje, wyłącznie do celów statystycznych, czy jest mikroprzedsiębiorstwem bądź małym lub średnim przedsiębiorstwem. I tak zgodnie z przepisami ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców:*

1) mikro przedsiębiorca – to przedsiębiorca, który w co najmniej jednym roku z dwóch ostatnich lat obrotowych spełniał łącznie następujące warunki: a) zatrudniał średniorocznie mniej niż 10 pracowników oraz b) osiągnął roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz z operacji finansowych nieprzekraczający równowartości w złotych 2 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczył równowartości w złotych 2 milionów euro;

2) mały przedsiębiorca – to przedsiębiorca, który w co najmniej jednym roku z dwóch ostatnich lat obrotowych spełniał łącznie następujące warunki: a) zatrudniał średniorocznie mniej niż 50 pracowników oraz b) osiągnął roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz z operacji finansowych nieprzekraczający równowartości w złotych 10 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczył równowartości w złotych 10 milionów euro, i który nie jest mikro przedsiębiorcą

3) średni przedsiębiorca – to przedsiębiorca, który w co najmniej jednym roku z dwóch ostatnich lat obrotowych spełniał łącznie następujące warunki: a) zatrudniał średniorocznie mniej niż 250 pracowników oraz b) osiągnął roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz z operacji finansowych nieprzekraczający równowartości w złotych 50 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczył równowartości w złotych 43 milionów euro, i który nie jest mikro przedsiębiorcą ani małym przedsiębiorcą.

4) jednoosobowa działalność gospodarcza - zorganizowana działalność zarobkowa, wykonywana we własnym imieniu i w sposób ciągły

5) osoba fizyczna nieprowadząca działalności gospodarczej- osoba fizyczna występująca w obrocie jako konsument, niebędąca przedsiębiorcą

Uwaga: Por. zalecenie Komisji z dnia 6 maja 2003 r. dotyczącego definicji przedsiębiorstw mikro, małych i średnich (notyfikowane jako dokument nr C(2003) 1422) (Dz.U. L 124 z 20.5.2003). Te informacje są wymagane wyłącznie do celów statystycznych.

Załącznik NR 2 do SWZ⁴

³ niepotrzebne skreślić

⁴ **Załącznik nr 2 do SWZ składa Wykonawca oraz jeżeli dotyczy, każdy z wykonawców wspólnie ubiegających się o zamówienie.**



Cyberbezpieczny Samorząd

Oświadczenie o braku podstaw do wykluczenia z postępowania

.....
(miejscowość, data)

Przystępując do postępowania w sprawie udzielenia zamówienia na:
Cyberbezpieczny Samorząd

działając w imieniu wykonawcy:
(podać nazwę i adres wykonawcy)

OŚWIADCZENIA DOTYCZĄCE WYKONAWCY

PKT 1.

Oświadczam, że na dzień składania ofert nie podlegam wykluczeniu z postępowania w zakresie art. 108 ust. 1 oraz art. 109 ust. 1 pkt 4 ustawy P.z.p.

PKT 2.

Oświadczam, że na dzień składania ofert, zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ustawy P.z.p. (podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 oraz art. 109 ust. 1 pkt 4 ustawy P.z.p.).

Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy P.z.p. podjąłem następujące środki naprawcze: (opisać)

PKT 3.

OŚWIADCZENIE DOTYCZĄCE DOSTĘPNOŚCI PODMIOTOWYCH ŚRODKÓW DOWODOWYCH:

Niżej podpisany(-a)(-i) oficjalnie wyraża(-ja) zgodę / nie wyraża(-ja) zgody** na to, aby Zamawiający uzyskał dostęp do dokumentów potwierdzających informacje, które zostały przedstawione w załączniku nr 2 do SIWZ na potrzeby niniejszego postępowania w zakresie podstawy wykluczenia o której mowa w art. 109 ust. 1 pkt. 4 ustawy P.z.p.. W przypadku wyrażenia zgody dokumenty te pobrać można pod adresami:

☐ <https://ems.ms.gov.pl/>

☐ <https://prod.ceidg.gov.pl/>;

W przypadku, gdy dokumenty te dostępne są pod innymi adresami niż powyżej podać należy np. adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji, identyfikator wydruku:

Załącznik NR 2a do SWZ⁵

⁵ Załącznik nr 2a do SWZ składa Wykonawca oraz każdy z wykonawców wspólnie ubiegających się o zamówienie, podmiot/-ty udostępniający/-ce swoje zasoby.



Cyberbezpieczny Samorząd

Oświadczenie wykonawcy, dotyczące podstaw wykluczenia 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.

Przystępując do postępowania w sprawie udzielenia zamówienia na:

Cyberbezpieczny Samorząd –

działając w imieniu wykonawcy:

(podać nazwę i adres wykonawcy)

OŚWIADCZENIA DOTYCZĄCE WYKONAWCY*

- ☐ Oświadczam, że na dzień składania ofert nie podlegam wykluczeniu 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***
- ☐ Oświadczam, że na dzień składania ofert, zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie ***art. 7 ust. 1 pkt.....(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w pkt 1, pkt 2, pkt 3.) ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.***

* wybrać odpowiednie

Załącznik **NR 3** do SWZ

Oświadczenie wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy, o braku przynależności do tej samej grupy kapitałowej



Cyberbezpieczny Samorząd

Przystępując do postępowania w sprawie udzielenia zamówienia na:
Cyberbezpieczny Samorząd –

Działając w imieniu wykonawcy:.....

(podać nazwę i adres wykonawcy)

Informuję, że*:

☐ nie należę

do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r. poz. 1076) co wykonawcy, którzy również złożyli oferty w powyższym postępowaniu.

☐ należę

do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r. poz. 1076), co wykonawca/y (nazwa i adres), który/rzy również złożył/li ofertę we wskazanym powyżej postępowaniu.

Jednocześnie wykazuję, iż złożona oferta została przygotowana niezależnie od oferty wskazanego powyżej wykonawcy: (wypełnić)

*Zaznaczyć odpowiednie.



Część II SWZ – Projekt umowy

Projekt umowy

Umowa Nr

W dniu pomiędzy

Miastem i Gminą Gołańcz, ul. dr. P. Kowalika 2, 62-130 Gołańcz zwaną dalej Zamawiającym, reprezentowaną przez:

mgr inż. Mieczysława Durskiego – Burmistrza Miasta i Gminy Gołańcz,

a

.....
zwanym dalej Wykonawcą, reprezentowanym przez:

.....
przy kontrasygnacie Pani Edyty Koniecznej – Skarbnika Miasta i Gminy Gołańcz
została zawarta umowa następującej treści:

§ 1. Przedmiot umowy

1. W wyniku dokonania przez Zamawiającego wyboru oferty Wykonawcy zgodnie z ustawą z dnia 11 września 2019 r. Prawo zamówień publicznych w trybie podstawowym bez negocjacji, Zamawiający zleca a Wykonawca przyjmuje do realizacji zadanie pod nazwą **Cyberbezpieczny Samorząd** w zakresie szczegółowo określonym w Specyfikacji Warunków Zamówienia.
2. Zadanie realizowane w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC). Celem tego programu jest wzmocnienie krajowego systemu cyberbezpieczeństwa, w szczególności poprzez zwiększenie poziomu bezpieczeństwa informacji w jednostkach samorządu terytorialnego. Numer umowy FERC.02.02-CS.01-001/23/2385.
3. Integralną częścią niniejszej Umowy są:
 - 1) Specyfikacja Warunków Zamówienia,
 - 2) Oferta Wykonawcy.

§ 2. Termin realizacji

1. Termin realizacji zamówienia ustala się **na 50 dni** licząc od dnia zawarcia niniejszej umowy.
2. Rozpoczęcie wykonywania przedmiotu umowy – **od dnia zawarcia umowy**.

§ 3. Obowiązki Wykonawcy

1. Wykonawca dostarczy urządzenia na swój koszt i ryzyko do siedziby urzędu tj. ul. Doktora Piotra Kowalika nr 2, 62-130 Gołańcz w terminie wskazanym w umowie. Przez termin dostawy rozumie się dzień, w którym Wykonawca dostarczy Zamawiającemu ostatnie z urządzeń wchodzących w skład Przedmiotu zamówienia, wolne od wad.
2. Na Wykonawcy ciąży odpowiedzialność z tytułu uszkodzenia lub utraty przedmiotu umowy, aż do chwili podpisania protokołu przekazania przez Zamawiającego.



Cyberbezpieczny Samorząd

3. Elementy składowe zestawów muszą być ze sobą kompatybilne, zapewnić bezproblemową współpracę, posiadać niezbędne elementy umożliwiające pracę urządzeń (w tym okablowanie).
4. Wykonawca zobowiązuje się dostarczyć przedmiot umowy fabrycznie nowy, bez wad wraz z aktualnymi atestami i certyfikatami bezpieczeństwa oraz wymaganiami norm.
5. Wykonawca dostarczy dokumentację techniczną na przedmioty: opis techniczny urządzeń, karty gwarancyjne, dokumenty potwierdzające zgodność urządzeń z normami jakościowymi i specyfikacją, instrukcje obsługi w języku polskim itp.
6. Zamawiający wymaga, aby dostarczany system operacyjny były fabrycznie nowy, nieużywany oraz nigdy wcześniej nieaktywowany na innym urządzeniu. Zamawiający wymaga, aby system operacyjny był zainstalowany (lub preinstalowany) fabrycznie na komputerach. Zamawiający wymaga, aby system operacyjny był dostarczony wraz ze stosownymi, oryginalnymi atrybutami legalności, np. certyfikatami autentyczności. Zamawiający nie dopuszcza rozwiązań licencyjnych wymagających stałych opłat w okresie użytkowania systemu operacyjnego.
7. **W dniu zawarcia Umowy Wykonawca złoży kosztorys, w którym zostaną wymienione wszystkie elementy przedmiotu zamówienia, w tym nazwa/model/marka, ilość, cena netto, stawka VAT, cena brutto.**
8. Wykonawca zobowiązany jest w dniu dostawy przekazać Zamawiającemu wszelką dokumentację dostarczoną przez producenta urządzeń, zgodnie z ofertą Wykonawcy, w szczególności: karty gwarancyjne, instrukcje obsługi w języku polskim (papierowe lub elektroniczne) oraz zapewni serwis i wsparcie techniczne – serwis obowiązkowo na terenie RP. Wykonawca dostarczy także wykaz dostarczonego sprzętu komputerowego z nr seryjnymi urządzeń.
9. Wykonawca zobowiązuje się do wywozu opakowań pozostałych po rozładunku przedmiotu zamówienia.

§ 3.

Sposób realizacji przedmiotu umowy

1. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, by nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
2. Wykonawca zobowiązany jest zgłosić pocztą elektroniczną na adres: informatyk@golancz.pl gotowość dostawy na co najmniej 2 dni robocze przed przewidywanym terminem dostawy.
3. Przy odbiorze przedmiotu zamówienia Zamawiający jest zobowiązany dokonać sprawdzenia ilości przedmiotu zamówienia. Odbioru ilościowego dostarczonego towaru dokonują w dniu dostawy wyznaczeni przedstawiciele Zamawiającego. Na potwierdzenie dokonania czynności zostanie sporządzony i podpisany przez każdą ze stron protokół odbioru.
4. O ile z umowy lub przepisów prawa nie wynika inaczej, jedynie podpisany przez obie Strony protokół odbioru jest podstawą do dokonania zapłaty wynagrodzenia. Zamawiający nie dopuszcza jednostronnych Protokołów odbioru wystawionych przez Wykonawcę.
5. Niezgodność jakościową dostarczonego przedmiotu zamówienia Zamawiający zobowiązany jest reklamować Wykonawcy na piśmie lub drogą elektroniczną w terminie 7 dni od dnia wykrycia wady i/lub usterki.
6. W przypadku reklamacji Wykonawca zobowiązuje się dostarczyć przedmiot zamówienia bez wad lub jego część w terminie 7 dni roboczych od dnia złożenia reklamacji.
7. Dokonanie odbioru urządzeń zgodnie z postanowieniami umowy nie zwalnia Wykonawcy od roszczeń z tytułu rękojmi lub gwarancji.
8. Językiem stosowanym w zapisach Umowy i językiem stosowanym podczas jej realizacji jest język polski. Dotyczy to także całej komunikacji między Stronami.
9. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.



10. Odbiór sprzętu objętego, zgodnie z SWZ i ofertą Wykonawcy, gwarancją producenta polegać będzie dodatkowo na sprawdzeniu okresu i warunków gwarancji na dedykowanej do tego stronie internetowej producenta lub innym kanałem udostępnionym przez producenta służącym do weryfikacji okresu i warunków gwarancji.
11. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.
12. Licencje na oprogramowanie zostaną udzielone zgodnie z postanowieniami OPZ.
13. Oferowane oprogramowanie musi pochodzić z oficjalnego kanału dystrybucji producenta.
14. Zamawiający zastrzega sobie możliwość weryfikacji legalności oprogramowania bezpośrednio u producenta w przypadku, jeśli poweźmie wątpliwości co do legalności jego pochodzenia.
15. Korzyści i ciężary związane ze sprzętem oraz niebezpieczeństwo przypadkowej utraty lub uszkodzenia sprzętu przechodzą na Zamawiającego z chwilą wydania sprzętu Zamawiającemu. Za dzień wydania sprzętu Zamawiającemu uważa się dzień, w którym sprzęt został odebrany przez Zamawiającego zgodnie z procedurą określoną w niniejszym paragrafie.

§ 4. Obowiązki i uprawnienia Zamawiającego

1. Zamawiający w trakcie realizacji postanowień niniejszej Umowy zobowiązuje się do bieżącej i stałej współpracy z Wykonawcą w celu zapewnienia wykonania przedmiotu Umowy zgodnie z jej postanowieniami, w szczególności do:
 - a) odbioru informacji przekazywanych przez Wykonawcę w związku z realizacją przedmiotu Umowy,
 - b) terminowej zapłaty wynagrodzenia Wykonawcy w okolicznościach uzasadniających jego wypłatę,

§5. Wynagrodzenie i sposób rozliczeń finansowych

1. Strony zgodnie postanawiają, iż określona przez Wykonawcę wartość wynagrodzenia ofertowego za wykonanie całości przedmiotu Umowy wyniesie nettozł (słownie złotych:), wraz z aktualnie obowiązującą stawką podatku VAT (brutto) wyniesiezł
2. Zamawiający dokona zapłaty na podstawie wystawionej faktury VAT, w terminie do 30 dni za wykonanie przedmiotu umowy, o którym mowa w § 1 niniejszej umowy na rachunek bankowy podany przez Wykonawcę. Zapłata nastąpi po podpisaniu protokołu odbioru końcowego przez Strony, przy czym za datę zapłaty uznaje się dzień wydania dyspozycji przelewu z rachunku bankowego Zamawiającego.
3. Zamawiający wymaga, aby do wystawionej przez Wykonawcę faktury została dołączona szczegółowa specyfikacja dostarczonego przedmiotu zamówienia. Specyfikacja powinna zawierać co najmniej: nazwę i opis dostarczonych towarów, ilość, jednostkę miary, cenę jednostkową netto, wartość netto, stawkę podatku VAT oraz wartość brutto. Dokument ten ma umożliwiać jednoznaczną weryfikację zgodności dostawy z przedmiotem zamówienia oraz kontrolę prawidłowości rozliczeń finansowych. Brak załączenia specyfikacji, o której mowa powyżej, może stanowić podstawę do wstrzymania płatności do czasu uzupełnienia wymaganej dokumentacji.



4. Wszelkie kwoty należne Zamawiającemu, w szczególności z tytułu kar umownych, mogą być potrącane z płatności realizowanych na rzecz Wykonawcy. W okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii ogłoszonego w związku z COVID-19, i przez 90 dni od dnia odwołania stanu, który obowiązywał jako ostatni, Zamawiający nie może potrącić kary umownej zastrzeżonej na wypadek niewykonania lub nienależytego wykonania umowy, z wynagrodzenia wykonawcy lub z innych jego wierzytelności, o ile zdarzenie, w związku, z którym zastrzeżono tę karę, nastąpiło w okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii.
5. W przypadku zmiany wysokości stawki podatku VAT za zrealizowanie dostawy stanowiącej przedmiot umowy, wynagrodzenie brutto, o którym mowa w ust. 1, ulega zmianie tak, aby dotychczasowe wynagrodzenie netto należne Wykonawcy nie uległo zmianie.

§ 6. Odstąpienie od umowy

1. Zamawiającemu przysługuje prawo odstąpienia od umowy w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy w terminie 30 dni od dnia powzięcia wiadomości o tych okolicznościach.
2. W przypadku, o którym mowa w ust.1 Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy, zrealizowanej od dnia odstąpienia umowy.
3. Zamawiający może odstąpić od Umowy ze skutkiem natychmiastowym również, gdy:
 - 1) Wykonawca nie wykonał dostawy w wyznaczonym terminie; stwierdzenia w toku odbioru przedmiotu umowy, że przedmiot umowy zawiera wady i pomimo wyznaczenia terminu ich usunięcia Wykonawca ich nie poprawił lub nie przystąpił do ich usunięcia;
 - 2) jeżeli Zamawiający nie współdziała z Wykonawcą w zakresie przewidzianym postanowieniami umowy, a współdziałanie to jest konieczne do wykonania Umowy, Wykonawca jest uprawniony do odstąpienia od umowy po uprzednim wezwaniu Zamawiającego do zapewnienia koniecznego współdziałania i wyznaczeniu mu w tym celu odpowiedniego terminu, nie krótszego niż 5 dni, z zagrożeniem odstąpienia od umowy w razie jego bezskutecznego upływu. W wezwaniu Wykonawca zobowiązany jest wskazać dokładnie brak wymaganego współdziałania i jego wpływ na realizację umowy. Wezwanie będzie wystosowane w formie pisemnej pod rygorem bezskuteczności wezwania.
4. Każda ze Stron może wypowiedzieć lub odstąpić od Umowy w razie zaistnienia przypadku siły wyższej, którego skutkiem jest niemożność wykonania obowiązków wynikających z Umowy przez którąkolwiek ze Stron przez okres ponad 15 dni. Po upływie wskazanego terminu każda ze Stron może wypowiedzieć lub odstąpić od Umowy ze skutkiem natychmiastowym i w drodze pisemnego oświadczenia przesłanego drugiej Stronie wraz z udowodnieniem tych okoliczności poprzez przedstawienie dokumentacji potwierdzającej wystąpienie zdarzeń mających cechy Siły wyższej oraz wskazania wpływu, jaki zdarzenie miało na przebieg realizacji umowy.
5. Przez pojęcie siły wyższej należy rozumieć zdarzenie zewnętrzne, którego nie można było przewidzieć, analizując i uwzględniając wszystkie okoliczności sprawy, jak również, któremu nie można było zapobiec znanymi, normalnie stosowanymi sposobami w szczególności zdarzenia o charakterze katastrofalnych działań przyrody albo nadzwyczajnych i zewnętrznych wydarzeń, którym zapobiec nie można, jak wojna przeciwko Rzeczypospolitej Polskiej lub działania zbrojne na terytorium Rzeczypospolitej Polskiej, terytorium państwa członkowskiego Unii Europejskiej, terytorium Państwa-Strony Traktatu Północnoatlantyckiego albo na terytorium innego państwa



Cyberbezpieczny Samorząd

graniczącego z Rzeczpospolitą Polską lub okupacja na tych terytoriach, restrykcje stanu wojennego, stanu wyjątkowego, powstania, rewolucji, zamieszek.

6. Odstąpienie od umowy dokonane przez którąkolwiek ze Stron powinno nastąpić w formie pisemnej pod rygorem nieważności oraz zawierać uzasadnienie.
7. W przypadku odstąpienia od umowy strony obciążają następujące obowiązki szczegółowe:
 - 1) w terminie 3 dni od daty odstąpienia od umowy Wykonawca przy udziale Zamawiającego sporządzi protokół inwentaryzacji dostarczonego sprzętu wg stanu na dzień odstąpienia od umowy;
8. Zamawiający w razie odstąpienia od umowy z przyczyn, za które odpowiada Zamawiający, zobowiązany jest do dokonania odbioru wyposażenia oraz do zapłaty wynagrodzenia za to wyposażenie, które zostało dostarczone do dnia odstąpienia.
9. Strony zgodnie postanawiają, że odstąpienie od umowy przez którąkolwiek ze Stron nie ma wpływu na obowiązki zapłaty zastrzeżonych kar umownych.

§ 7 Gwarancja jakości i rękojmia za wady

1. Wykonawca udziela minimum 36-miesięcznej gwarancji z opcją door-to-door na przedmiot umowy – zgodnie z warunkami przedstawionymi w ofercie i niniejszej umowie.
2. Wykonawca udzieli gwarancji dla dostarczonego serwera na następujących warunkach:
 - a) Gwarancja: minimum 5 lat w trybie Next Business Day;
 - b) Opcja serwisowa zachowania dysków twardych – minimum 5 lat.
3. Realizacja obowiązków gwarancyjnych przez Wykonawcę będzie się odbywała na następujących warunkach:
 - a) okres gwarancji liczony jest od daty podpisania protokołu odbioru bez uwag;
 - b) gwarancja obejmuje bezpłatne naprawy, a w przypadku braku możliwości naprawy wymianę towaru lub jego podzespołu na nowy i ewentualnie poniesienie kosztów transportu;
 - c) Wykonawca, w okresie gwarancyjnym, zapewni bezpłatny dojazd serwisanta do Zamawiającego, bezpłatny transport sprzętu do i z serwisu.
 - d) w okresie gwarancji serwis dostarczonego sprzętu będzie realizowany nieodpłatnie;
 - e) Wykonawca zapewni autoryzowany serwis gwarancyjny przez okres gwarancji;
 - f) zgłoszenie następuje pocztą elektroniczną pod adresem lub pod numerem telefonu ;
 - g) osobą odpowiedzialną ze strony Wykonawcy do kontaktu z Zamawiającym w sprawach serwisu gwarancyjnego jest Pan/Pani ;
 - h) Wykonawca ze swej strony zobowiązuje się do usunięcia stwierdzonej w okresie gwarancji wady nieodpłatnie na swój koszt w terminie do 14 dni od daty zgłoszenia, chyba że nie będzie to możliwe z przyczyn niezależnych od Wykonawcy. W takim przypadku Strony ustalą inny termin usunięcia wad. W razie nieusunięcia wad w wyznaczonym terminie, Zamawiający ma prawo do zastępczego usunięcia wad w formie naprawy lub wymiany towaru lub jego podzespołu na nowy w ramach gwarancji na koszt Wykonawcy;
 - i) jeżeli w wykonaniu obowiązków wynikających z gwarancji Wykonawca dokonał napraw towaru lub nastąpiła wymiana towaru objętego gwarancją lub jego istotnego podzespołu na nowy, termin gwarancji biegnie na nowo od dnia protokolarnego odbioru naprawionego lub wymienionego sprzętu;
 - j) maksymalnie 3 udokumentowane naprawy gwarancyjne tego samego sprzętu, wyłączające dany sprzęt z eksploatacji uprawniają do zadania wymiany sprzętu na nowy;
 - k) Wykonawca nie może odmówić usunięcia wad lub wymiany towaru lub jego podzespołów bez względu na wysokość związanych z tym kosztów;
 - l) odpowiedzialność z tytułu gwarancji obejmuje zarówno wady powstałe z przyczyn tkwiących w sprzęcie w chwili dokonania jego odbioru przez Zamawiającego, jak i wszystkie inne wady



Cyberbezpieczny Samorząd

fizyczne towaru, powstałe z przyczyn, za które Wykonawca ponosi odpowiedzialność, pod warunkiem, że wady te ujawnią się w ciągu terminu obowiązywania gwarancji;

m) Zamawiający może dochodzić roszczeń z tytułu gwarancji także po upływie gwarancji, jeśli wniósł reklamację przed upływem okresu gwarancji.

4. Warunki gwarancji określają dokumenty gwarancyjne przekazane Zamawiającemu wraz z protokołem odbioru oraz niniejsza umowa. W przypadku rozbieżności postanowień w danej kwestii pierwszeństwo mają postanowienia korzystniejsze dla Zamawiającego.
5. Gwarancja udzielona przez Wykonawcę nie wyłącza uprawnień Zamawiającego z tytułu gwarancji udzielonych przez producentów sprzętu. Warunki gwarancji mają pierwszeństwo przed warunkami gwarancji udzielonymi przez producentów sprzętu w zakresie, w jakim przyznają Zamawiającemu silniejszą ochronę.
6. W przypadku, gdy z kart gwarancyjnych wynikają korzystniejsze warunki gwarancji niż przewidziane powyżej mają one zastosowanie do niniejszej Umowy.

§ 8. Kary umowne

1. Wykonawca zapłaci Zamawiającemu kary umowne:
 - a) za zwłokę w dostarczeniu przedmiotu umowy w całości, w wysokości 0,1% całkowitego wynagrodzenia brutto należnego Wykonawcy, określonego w § 5 ust. 1 Umowy, za każdy dzień zwłoki, licząc od dnia upływu terminu dostawy określonego w umowie;
 - b) za zwłokę w usunięciu wad zgłoszonych reklamacją bądź obowiązków gwarancyjnych w wysokości 0,1% całkowitego wynagrodzenia brutto należnego Wykonawcy, określonego w § 5 ust. 1 Umowy za każdy dzień zwłoki;
 - c) za zwłokę w realizacji obowiązków gwarancyjnych w wysokości 0,1% całkowitego wynagrodzenia brutto należnego Wykonawcy, określonego w § 5 ust. 1 Umowy za każdy dzień zwłoki;
 - d) za odstąpienie od umowy z przyczyn zależnych od Wykonawcy w kwocie 10 % wynagrodzenia brutto określonego w § 5 ust. 1 umowy
2. Kary umowne liczone są od wynagrodzenia brutto należnego Wykonawcy.
3. O nałożeniu kary umownej, jej wysokości i podstawie jej nałożenia Zamawiający będzie informował Wykonawcę pisemnie w terminie 7 dni od zaistnienia zdarzenia.
4. Zapłata kar umownych przez Wykonawcę nie zwalnia go z jakichkolwiek innych obowiązków i zobowiązań umownych.
5. W przypadku wystąpienia szkody, której wysokość przekracza wysokość zastrzeżonych kar umownych Strony uprawnione są do dochodzenia odszkodowania przekraczającego wysokość kar umownych zasadach na ogólnych ustawy Kodeks cywilny.
6. W przypadku odstąpienia Zamawiającego od umowy niespowodowanego winą Wykonawcy zapłaci on Wykonawcy 10% całości wynagrodzenia brutto określonego w §5 ust. 1, za wyjątkiem sytuacji opisanej w art. 456 ust. 1 ustawy Prawo zamówień publicznych
7. Potrącenie kar umownych nastąpi z przysługującego Wykonawcy wynagrodzenia.
8. Kary umowne stają się wymagalne w pierwszym dniu, kiedy możliwe jest ich naliczenie, a w przypadku kar za zwłokę z każdym dniem.
9. Łączna wysokość kar umownych nie może przekroczyć kwoty 40% wynagrodzenia brutto określonego w §5 ust 1 Umowy.



§ 9. Zmiany postanowień umowy

1. Strony przewidują zmianę umowy w przypadku:
 - 1) zmian koniecznych, spowodowanych okolicznościami, których Zamawiający, działając z należytą starannością nie mógł przewidzieć;
 - 2) zmiany wynagrodzenia wskutek zmiany urzędowej stawki podatku VAT,
2. Zamawiający dopuszcza możliwość zmiany umowy we wszystkich jej zakresach (w tym w zakresie terminu realizacji, wynagrodzenia wykonawcy, zakresu przedmiotowego, sposobu płatności) także w przypadku wystąpienia następujących okoliczności:
 - 1) trwania wojny napastniczej przeciwko Rzeczypospolitej Polskiej lub działań zbrojnych na terytorium Rzeczypospolitej Polskiej, terytorium państwa członkowskiego Unii Europejskiej, terytorium Państwa-Strony Traktatu Północnoatlantyckiego albo na terytorium innego państwa graniczącego z Rzeczpospolitą Polską lub okupacji na tych terytoriach lub
 - 2) obowiązywania na obszarze Rzeczypospolitej Polskiej stanu klęski żywiołowej, stanu wyjątkowego albo stanu wojennego,
 - strony umowy dopuszczają zmianę umowy w zakresie, o którym mowa w ust. 1, jeśli powyższe okoliczności mają wpływ na należyte wykonanie umowy.
3. Strony umowy wzajemnie informują się o wpływie okoliczności, o których mowa w ust. 2 na należyte wykonanie umowy potwierdzając ten wpływ oświadczeniami lub dokumentami.
4. Każda ze stron umowy może żądać przedstawienia dodatkowych oświadczeń lub dokumentów potwierdzających wpływ okoliczności, o których mowa w ust. 2 na należyte wykonanie tej umowy.
5. Zamawiający, po stwierdzeniu, że okoliczności, o których mowa w ust. 2, wpływają na należyte wykonanie umowy, w uzgodnieniu z wykonawcą dokonuje zmiany umowy, o której mowa w art. 455 ust. 1 pkt 4 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych, przez:
 - 1) zmianę terminu wykonania umowy lub jej części, lub czasowe zawieszenie wykonywania umowy lub jej części,
 - 2) zmianę sposobu wykonywania dostaw, usług lub robót budowlanych,
 - 3) zmianę zakresu świadczenia wykonawcy i odpowiadającą jej zmianę wynagrodzenia lub sposobu rozliczenia wynagrodzenia wykonawcy,
 - o ile wzrost wynagrodzenia spowodowany każdą kolejną zmianą nie przekroczy 50% wartości pierwotnej umowy.
6. Dokonywanie wszelkich zmian dotyczących niniejszej umowy wymaga formy pisemnej pod rygorem nieważności.
7. Nie stanowi zmiany Umowy zmiana danych rejestrowych lub adresowych oraz danych kontaktowych.
8. Zamawiający zastrzega, iż jeśli w wyniku wprowadzenia zmian do umowy, o których mowa w § 9 dojdzie do ograniczenia zakresu zamówienia przez Zamawiającego, minimalna wartość lub wielkość świadczenia stron wynosi 75% wartości Zamówienia.

§ 9¹

(zmiana umowy w związku z występowaniem stanu epidemii lub zagrożenia epidemicznego.)

1. Zamawiający dopuszcza możliwość zmiany umowy we wszystkich jej zakresach (w tym w zakresie terminu realizacji, wynagrodzenia wykonawcy, zakresu przedmiotowego, sposobu płatności) w przypadku występowania okoliczności utrudniających lub uniemożliwiających realizację zamówienia (lub dopiero mających taki stan wywołać) w związku z występowaniem stanu epidemii lub zagrożenia epidemicznego.
2. Strony niezwłocznie informują się wzajemnie o wpływie okoliczności związanych z wystąpieniem stanu epidemii lub zagrożenia epidemicznego na należyte wykonanie niniejszej umowy, o ile taki wpływ wystąpił lub może wystąpić. Strony umowy potwierdzają ten wpływ,



Cyberbezpieczny Samorząd

dołączając do informacji, o której mowa w zdaniu pierwszym, oświadczenia lub dokumenty, które mogą dotyczyć w szczególności:

- 1) nieobecności pracowników lub osób świadczących pracę za wynagrodzeniem na innej podstawie niż stosunek pracy, które uczestniczą lub mogłyby uczestniczyć w realizacji zamówienia z uwagi na: ich obowiązkową hospitalizację, objęcie kwarantanną lub nadzorem epidemiologicznym w związku z pozostawaniem w styczności z osobami, których zdrowie zostało zagrożone, zwolnienie od wykonywania pracy z powodu konieczności osobistego sprawowania opieki nad dzieckiem, o którym mowa w art. 32 ust. 1 pkt 1 ustawy z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa, lub dzieckiem legitymującym się orzeczeniem o znacznym lub umiarkowanym stopniu niepełnosprawności do ukończenia 18 lat albo dzieckiem z orzeczeniem o niepełnosprawności w przypadku zamknięcia żłobka, klubu dziecięcego, przedszkola, szkoły lub innej placówki, do których uczęszcza dziecko, lub niemożności sprawowania opieki przez nianię lub dziennego opiekuna z powodu stanu epidemii lub zagrożenia epidemicznego.
 - 2) decyzji wydanych przez Głównego Inspektora Sanitarnego lub działającego z jego upoważnienia państwowego wojewódzkiego inspektora sanitarnego nakładających na wykonawcę obowiązek podjęcia określonych czynności zapobiegawczych lub kontrolnych;
 - 3) poleceń lub decyzji wydanych przez wojewodów, ministra właściwego do spraw zdrowia lub Prezesa Rady Ministrów;
 - 4) wstrzymania lub trudności w zakresie realizacji dostaw produktów, komponentów produktu lub materiałów niezbędnych do realizacji przedmiotu umowy,
 - 5) trudności w dostępie do sprzętu lub trudności w realizacji usług transportowych;
 - 6) innych okoliczności, które uniemożliwiają bądź w istotnym stopniu ograniczają możliwość wykonania umowy;
 - 7) okoliczności, o których mowa w pkt 1-6, w zakresie w jakim dotyczą one podwykonawcy lub dalszego podwykonawcy.
- 2a. W przypadku wykonawców mających siedzibę lub wykonujących działalność związaną z realizacją umowy poza terytorium Rzeczypospolitej Polskiej, w miejsce dokumentów, o których mowa w ust. 1 pkt 1-6, składa się dokumenty wydane przez odpowiednie instytucje w tych krajach lub oświadczenia tych wykonawców.
3. Każda ze stron może żądać przedstawienia dodatkowych oświadczeń lub dokumentów potwierdzających wpływ okoliczności związanych z wystąpieniem stanu epidemii lub zagrożenia epidemicznego na należyte wykonanie tej umowy.
 4. Zamawiający po stwierdzeniu, że okoliczności związane z wystąpieniem stanu epidemii lub zagrożenia epidemicznego o których mowa w ust. 2, wpływają na należyte wykonanie umowy w uzgodnieniu z wykonawcą dokonuje zmiany umowy, w szczególności przez:
 - 1) zmianę terminu wykonania umowy lub jej części, lub czasowe zawieszenie wykonywania umowy lub jej części,
 - 2) zmianę sposobu wykonywania dostawy sprzętu wraz z jego wdrożeniem w siedzibie (serwerowni) Zamawiającego.
 - 3) zmianę zakresu świadczenia Wykonawcy i odpowiadającą jej zmianę wynagrodzenia Wykonawcy,- o ile wzrost ceny spowodowany każdą kolejną zmianą nie przekroczy 50% wartości pierwotnej umowy.



Cyberbezpieczny Samorząd

5. W przypadku stwierdzenia, że okoliczności związane z wystąpieniem stanu epidemii lub zagrożenia epidemicznego, o których mowa w ust. 2, mogą wpłynąć na należyte wykonanie umowy, zamawiający, w uzgodnieniu z wykonawcą, może dokonać zmiany umowy zgodnie z ust. 4.
6. Zmiana terminu wykonania umowy lub jej części, lub czasowe zawieszenie wykonywania umowy lub jej części może nastąpić wyłącznie o czas trwania przeszkody i/lub o czas trwania skutków związanych z wystąpieniem tej przeszkody.
7. Strona wnioskująca o zmianę umowy przedstawia wpływ okoliczności związanych z wystąpieniem stanu epidemii lub zagrożenia epidemicznego na należyte jej wykonanie.
8. Wykonawca i podwykonawca, po stwierdzeniu, że okoliczności związane z wystąpieniem stanu epidemii lub zagrożenia epidemicznego, mogą wpłynąć lub wpływają na należyte wykonanie łączącej ich umowy, która jest związana z wykonaniem zamówienia publicznego lub jego części, uzgadniają odpowiednią zmianę tej umowy, w szczególności mogą zmienić termin wykonania umowy lub jej części, czasowo zawiesić wykonywanie umowy lub jej części, zmienić sposób wykonywania umowy lub zmienić zakres wzajemnych świadczeń
9. W przypadku dokonania zmiany umowy, jeżeli zmiana ta obejmuje część zamówienia powierzoną do wykonania podwykonawcy, wykonawca i podwykonawca uzgadniają odpowiednią zmianę łączącej ich umowy, w sposób zapewniający, że warunki wykonania tej umowy przez podwykonawcę nie będą mniej korzystne niż warunki wykonania umowy zmienionej pomiędzy Zamawiającym a Wykonawcą.

§ 10. Komunikacja między Stronami

1. Strony zobowiązują się do wzajemnego informowania się o zmianach danych kontaktowych, teleadresowych oraz innych istotnych zmianach, mogących mieć wpływ na prawidłowy przebieg realizacji umowy.
2. Komunikacja między stronami następować będzie drogą elektroniczną (w tym e-mailową), telefoniczną, pisemną, pocztową lub faksem.
3. Strony ustalają następujące dane kontaktowe na potrzeby realizacji umowy:
 - 1) **dane Zamawiającego:**
 - a) osoba do kontaktu:,
 - b) adres do korespondencji pocztowej:,
 - c) adres do korespondencji elektronicznej:,
 - d) telefon kontaktowy:,
 - e) fax:
 - 2) **dane Wykonawcy:**
 - a) osoba do kontaktu:,
 - b) adres do korespondencji pocztowej:,
 - c) adres do korespondencji elektronicznej:,
 - d) telefon kontaktowy:,
 - e) fax:
4. Zmiana osób i ich danych wskazanych w ust. 3 następuje w formie pisemnej pod rygorem nieważności. Za równoważny uznaje się dokument z podpisem elektronicznym przesłany drogą mailową do Zamawiającego. Zmiana tych danych nie wymaga zawarcia aneksu do umowy.

§ 11. Postanowienia końcowe

1. W sprawach nieuregulowanych niniejszą umową stosuje się, w szczególności przepisy Prawa zamówień publicznych i Kodeksu cywilnego.
2. Strony podają jako adresy do korespondencji adresy wskazane we wstępie do niniejszej umowy.



Cyberbezpieczny Samorząd

Każda ze stron zobowiązana jest do pisemnego powiadomienia drugiej strony o zmianie adresu. W przypadku zaniechania zawiadomienia skuteczne jest skierowanie oświadczenia na ostatni znany drugiej stronie adres.

3. Właściwym do rozpoznania sporów mogących wynikać na tle realizacji umowy jest sąd powszechny właściwy miejscowo dla Zamawiającego.
4. Umowę niniejszą sporządza się w trzech egzemplarzach, dwa egzemplarze dla Zamawiającego i jeden egzemplarz dla Wykonawcy.

Załączniki:

1. *Specyfikacja Warunków Zamówienia, w tym opis przedmiotu zamówienia,*
2. *Oferta Wykonawcy.*

Z a m a w i a j ą c y

W y k o n a w c a

K o n t r a s y g n a t a