

Wielka Nieszawka, dn. 27.03.2025 r.

RIT.271.2.4.4.2025.MR

Specyfikacja Warunków Zamówienia

na wykonanie zadania:

Dostawa sprzętu, oprogramowania oraz usług informatycznych w ramach Projektu grantowego „Cyberbezpieczny Samorząd”

Postępowanie o udzielenie zamówienia publicznego prowadzone w trybie podstawowym na podstawie ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320), o wartości szacunkowej niższej niż kwoty określone w przepisach, o których mowa w art. 3 ustawy Pzp

Specyfikację zatwierdził:

Wójt Gminy Wielka Nieszawka

Katarzyna Streich

Spis treści

Rozdział 1. Informacje o Zamawiającym	3
Rozdział 2. Tryb udzielenia zamówienia publicznego	3
Rozdział 3. Opis przedmiotu zamówienia	3
Rozdział 4. Termin wykonania zamówienia	53
Rozdział 5. Podwykonawstwo	54
Rozdział 6. Korzystanie przez Wykonawcę ze zdolności technicznych lub sytuacji ekonomicznej innych podmiotów	54
Rozdział 7. Oferta składana przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia	55
Rozdział 8. Opis warunków udziału w postępowaniu i podstawy wykluczenia.	56
Podstawy wykluczenia	56
Rozdział 9. Oświadczenia i dokumenty, jakie zobowiązani są dostarczyć wykonawcy w celu potwierdzenia spełniania warunków udziału w postępowaniu oraz wykazania braku podstaw wykluczenia (podmiotowe środki dowodowe)	58
Rozdział 10. Informacje o sposobie porozumiewania się zamawiającego z Wykonawcami oraz przekazywania oświadczeń lub dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z wykonawcami	60
Rozdział 11. Wyjaśnienia treści SWZ	62
Rozdział 12. Opis sposobu przygotowania Ofert	62
Rozdział 13. Wadium	64
Rozdział 14. Termin związania Ofertą	64
Rozdział 15. Miejsce i termin składania i otwarcia Ofert	64
Rozdział 16. Sposób obliczania ceny	65
Rozdział 17. Sposób oceny kryteriów wyboru Oferty	66
Rozdział 18. Formalności, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia Umowy	67
Rozdział 19. Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do treści tej umowy	67
Rozdział 20. Środki ochrony prawnej	67
Rozdział 21. Postanowienia końcowe	68
Załączniki do SWZ:	68

ROZDZIAŁ 1. INFORMACJE O ZAMAWIAJĄCYM

Nazwa: **GMINA WIELKA NIESZAWKA**
Adres: **ul. Toruńska 12, 87-165 Cierpice**
Numer telefonu: **56/ 678 12 12**
Adres poczty elektronicznej: **sekretariat@wielkanieszawka.pl**
Adres strony internetowej prowadzonego postępowania: **<https://platformazakupowa.pl/transakcja/1082177>**

ROZDZIAŁ 2. TRYB UDZIELENIA ZAMÓWIENIA PUBLICZNEGO

1. Postępowanie prowadzone jest w trybie podstawowym na podstawie art. 275 ust. 1 ustawy Pzp.
2. Wartość szacunkowa zamówienia nie przekracza progów unijnych, o których mowa w art. 3 ustawy Pzp.
3. Zamawiający dopuszcza składanie ofert częściowych.
4. Postępowanie prowadzone jest w języku polskim.
5. Zamawiający nie dopuszcza składania ofert wariantowych.
6. Zamawiający nie przewiduje udzielania zamówień, o których mowa w art. 214 ust. 1 pkt 7 i 8 ustawy Pzp.
7. Zamawiający nie przewiduje zawarcia umowy ramowej.
8. Zamawiający nie przewiduje zastosowania aukcji elektronicznej.
9. Zamawiający nie dopuszcza składania ofert w postaci katalogów elektronicznych.
10. Zamawiający nie zastrzega możliwości ubiegania się o udzielenie zamówienia wyłącznie przez wykonawców, o których mowa w art. 94 ustawy Pzp.
11. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu, z zastrzeżeniem art. 261.
12. Ogłoszenie i Specyfikacja Warunków Zamówienia (SWZ) udostępnione zostaną na platformie zakupowej OPEN NEXUS pod adresem: <https://platformazakupowa.pl/transakcja/1082177> od dnia publikacji ogłoszenia o zamówienia w Biuletynie Zamówień Publicznych, nie krócej niż do dnia udzielenia zamówienia. Na tej stronie będą również udostępnione zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia.
13. Zamawiający w oparciu o art. 100 ust. 1 ustawy Pzp wymaga, aby prowadzone dostawy umożliwiły swobodne i bezpieczne poruszanie się osobom niepełnosprawnym (sposób realizacji dostaw winien zapewniać w pełni dostępność i bezpieczeństwo tym osobom).
14. Zamawiający nie wymaga dokonania przez Wykonawcę wizji lokalnej, o której mowa w art. 131 ust. 2 ustawy Pzp.
15. Zadanie realizowane z projektu „Cyberbezpieczny Samorząd” dofinansowanego w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa”.

ROZDZIAŁ 3. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest **Dostawa sprzętu, oprogramowania oraz usług informatycznych** realizowane w ramach projektu grantowego „Cyberbezpieczny Samorząd”.

LP.	OPIS	ILOŚĆ
CZĘŚĆ I		
	URZĄD GMINY W WIELKIEJ NIESZAWCE [UG]	
1.	UTM Zapora sieciowa	1 szt.
CZĘŚĆ II		
	REALIZACJA W RAMACH ETAPU I	
	GMINNY OŚRODEK POMOCY SPOŁECZNEJ [GOPS]	
1.	Zasilacz awaryjny – UPS 850VA	5 szt.
2.	Zasilacz awaryjny – UPS 1200VA	1 szt.
	REALIZACJA W RAMACH ETAPU II	
	URZĄD GMINY W WIELKIEJ NIESZAWCE [UG]	
1.	Zasilacz awaryjny – UPS 850VA	16 szt.
2.	Zasilacz awaryjny – UPS 1600VA	1 szt.
CZĘŚĆ III		
	REALIZACJA W RAMACH ETAPU I	
	GMINNY OŚRODEK POMOCY SPOŁECZNEJ [GOPS]	
1.	Serwer 1	1 szt.
2.	Serwer 2	1 szt.
3.	Oprogramowanie oraz monitoring usług i użytkowanych systemów	1 szt.
	REALIZACJA W RAMACH ETAPU II	
	URZĄD GMINY W WIELKIEJ NIESZAWCE [UG]	
1.	System umożliwiający monitoring komputerów	1 szt.
2.	Oprogramowanie oraz monitoring usług i użytkowanych systemów	1 szt.
CZĘŚĆ IV		
	REALIZACJA W RAMACH ETAPU I	
	GMINNY OŚRODEK POMOCY SPOŁECZNEJ [GOPS]	
1.	Usługa chmurowa dla backup baz danych	1 szt.
	REALIZACJA W RAMACH ETAPU II	
	URZĄD GMINY W WIELKIEJ NIESZAWCE [UG]	
1.	Usługa chmurowa dla backup baz danych	1 szt.
CZĘŚĆ V		
	URZĄD GMINY W WIELKIEJ NIESZAWCE [UG]	
1.	System backup	1 szt.
2.	Punkty dostępowe	2 szt.
	REALIZACJA W RAMACH ETAPU II	
	URZĄD GMINY W WIELKIEJ NIESZAWCE [UG]	
1.	Oprogramowanie antywirusowe	1 szt.

2. Szczegółowy opis przedmiotu zamówienia:

CZĘŚĆ I

URZĄD GMINY W WIELKIEJ NIESZAWCE

I.UG.1 UTM Zapora sieciowa - Firewall w klastrze active/passive

Parametr	charakterystyka [wymagania minimalne]
----------	---------------------------------------

Funkcje modułu Firewall:

1. Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).
2. Możliwość uruchomienia w formie klastra wysokiej dostępności (HA) - co najmniej Active-Passive.
3. Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).
4. Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.
5. Musi obsługiwać Multicast routing.
6. Musi obsługiwać Policy Based routing.
7. Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.
8. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
9. Musi obsługiwać DHCPv6 na zewnętrznym interfejsie.
10. Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).
11. Musi obsługiwać Dynamic DNS.
12. Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
13. Musi obsługiwać translację portów: PAT.
14. Musi obsługiwać IPSec NAT traversal.
15. Musi obsługiwać mechanizm Policy Based NAT.
16. Musi obsługiwać VLAN 802.1Q.
17. Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
18. Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.
19. Musi mieć możliwość obsługi zapasowego łącza typu 4G LTE/5G poprzez podłączenie zewnętrznego modemu USB.
20. Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.
21. Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.
22. Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza, minimum dla wartości: utrata pakietów, opóźnienie, jitter.
23. Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
24. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
25. Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.
26. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.
27. Musi posiadać co najmniej dwie metody transparentnej autoryzacji nie wymagające instalacji dedykowanego agenta na stacjach roboczych użytkowników.
28. Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.

Specyfikacja UTM:

Dostarczony system bezpieczeństwa (UTM) musi zapewniać:

29. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
 30. Musi dostarczać mechanizm identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
 31. Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
 32. Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
 33. Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.
 34. Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
 35. Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.
 36. Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMTPS, POP3S, IMAPS, H.323, SIP.
 37. Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.
 38. Musi zapewniać funkcjonalność TLS/SSL Offloading dla protokołu HTTPS w ramach połączeń do wewnętrznych serwerów.
 39. Musi ochraniać przed minimum: atakami DoS, pofragmentowanymi i zniekształconymi pakietami, zagrożeniami mieszanymi (Blended threats).
 40. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.
 41. VPN site-to-site musi wspierać minimum: IKEv2, IPSec, tunele oparte na politykach i routingu, TLS hub and spoke.
 42. VPN client-to-site musi wspierać minimum: IKEv2, IPSec, L2TP, TLS
1. Firewall musi zapewnić obsługę na poziomie minimalnym: 4.96 Gbps dla pracy w trybie firewall, 943 Mbps dla pracy w trybie full scan (włączone mechanizmy bezpieczeństwa takie jak: AV, IPS)
 2. Ilość obsługiwanych sieci VLAN: 75
 3. Firewall musi obsługiwać 3 850 000 jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną 35 500 połączeń na sekundę.
 4. Minimalna ilość portów 10/100/1000 BaseT: 8
 5. Możliwość rozszerzenia portów o dodatkowy port 1x SFP+ lub 4G/LTE.
 6. Wsparcie połączeń VPN site-to-site lub client-to-site dla minimum 60 użytkowników.
1. Ochronę z wykorzystaniem mechanizmów IPS.
 2. Ochronę antywirusową.
 3. Ochronę przed niechcianą pocztą.
 4. Kontrolę wykorzystywanych aplikacji.

W ramach ochrony przed atakami system musi zapewniać:

W ramach kontroli antywirusowej system musi zapewniać:

W ramach kontroli antyspamowej system musi zapewniać:

W ramach filtrowania zawartości URL system musi zapewniać:

5. Możliwość filtrowania URL.

1. Automatyczną aktualizację bazy sygnatur IPS. Powinna ona zawierać co najmniej 8000 definicji sygnatur.
2. Automatyczne blokowanie znanych źródeł ataków.
3. Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.
4. Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).
5. Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer Overflow, Remote File Inclusions.
6. Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.

1. Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bez sygnaturowej lokalnie
2. Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.
3. Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.
4. Możliwość skanowania plików o rozmiarze co najmniej 10MB.
5. Możliwość zdefiniowania rozmiaru skanowanego pliku.
6. Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.
7. Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.
8. Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Ransomware, Malware.
9. Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.

1. Analizę wiadomości pocztowych w oparciu o technologię Recurrent Pattern Detection.
2. Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.
3. Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.
4. Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.
5. Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.

1. Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.
2. Baza filtra url powinna zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.
3. Odpytywanie bazy on-line w czasie rzeczywistym.
4. Możliwość wystania modyfikowalnej notyfikacji do użytkownika o tym, dlaczego dostęp do strony www został zablokowany.
5. Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.
6. Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.

W ramach kontroli aplikacyjnej system musi zapewniać:

Wymagane funkcje VPN systemu:

Zarządzanie

7. Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.
8. Możliwość określenia różnego rodzaju akcji dla połączeń do wybranych adresów URL na podstawie reputacji.
9. Możliwość filtrowania treści w oparciu o typy MIME.
10. Możliwość blokowania plików cookies dla określonych domen.
11. Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
12. Analizę treści dla protokołu https.
13. Wyłączenie inspekcji https dla wybranych kategorii stron www.

1. Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
2. Ilość rozpoznawanych aplikacji: nie mniej niż 1000, podzielonych na kategorie.
3. W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).
4. Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.

1. Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.
2. W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.
3. Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
4. Musi wspierać mechanizmy uwierzytelniania: SHA-2, MD5, IKE Pre-Shared Key, certyfikaty.
5. Obsługa Dead Peer Detection (DPD).
6. Wsparcie dla IKEv1 i IKEv2.
7. Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.
8. Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).
9. Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.
10. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.
11. Połączenia client-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.
12. Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.

1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.
2. Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
3. Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
4. W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).

Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania:

5. Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.
 6. Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.
 7. Komunikacja do systemów logowania i raportowania musi być szyfrowana.
 8. W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania.
1. Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.
 2. Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.
 3. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online
 4. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline
 5. Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
 6. Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
 7. System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
 8. Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
 9. System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.
 10. Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
 11. Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.
 12. Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.
 13. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
 14. Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.
 15. Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.
 16. System ma mieć możliwość generowania raportów w formacie PDF oraz opcję eksportowania szczegółowych informacji do pliku CSV.
 17. System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.
 18. Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
 19. System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
 20. System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.

Wsparcie techniczne

21. Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urzędzeń poszczególnym użytkownikom.

22. Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów.

Gwarancja producenta i wsparcie techniczne - nie później niż do 30.06.2026r.

CZĘŚĆ II

REALIZACJA W RAMACH ETAPU I

GMINNY OŚRODEK POMOCY SPOŁECZNEJ

II.I.GOPS.1 Zasilacz awaryjny UPS 850VA

Parametr	charakterystyka [wymagania minimalne]
moc pozorna	min. 850VA
moc rzeczywista	min. 480W
Typ obudowy	wolnostojąca
Napięcie wejściowe	$\sim 170 \div 280 \text{ V AC} \pm 7 \%$
Częstotliwość napięcia wejściowego	45 - 55Hz $\pm 1\text{Hz}$
Zakres napięcia wyjściowego	230 V AC $\pm 10 \%$
Progi przetaczania sieć – UPS	$\sim 170 \div 280 \text{ V AC} \pm 7 \%$
Czas przetaczania sieć – UPS	<6ms
Napięcie wyjściowe	$\sim 230\text{V} \pm 5\%$
Częstotliwość napięcia wyjściowego	50Hz $\pm 1\text{Hz}$
Kształt napięcia wyjściowego na pracy rezerwowej	Schodkowa aproksymacja sinusoidy
Progi przetaczania UPS – sieć	$\sim 176 \text{ V} \div 274 \text{ V AC} \pm 7 \%$
Zabezpieczenie przeciwzwarciowe	elektroniczne
Zabezpieczenie przeciążeniowe	elektroniczne
Czas podtrzymania (P1,0/0,8max/P0,5max)	minimum 2/6 min
akumulatory wewnętrzne	minimum 1 szt 12V9Ah; szczelne, bezobsługowe
Ilość i typ gniazd wyjściowych	minimum 2 standardu polskiego określone w normach PN-E-93201:1997 i PN-IEC 60884:2006
Sygnalizacja	diodowa, wskazująca pracę sieciową, baterijną, przeciążenie i ładowanie akumulatora
oprogramowanie	wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, wymagane wsparcie producenta w języku polskim odnośnie konfiguracji i rozwiązywania problemów. oprogramowanie do zarządzania i monitorowania pracy UPS w języku polskim, do pobrania ze strony producenta
Gwarancja oraz serwis	minimum 36 miesięcy na elektronikę i 24 miesiące na akumulatory; autoryzowany serwis producenta zlokalizowany w Polsce. serwis realizowany w systemie door to door

na Rozwój Cyfrowy

Certyfikaty, oświadczenia (należy dołączyć do oferty)

- deklaracja CE producenta sprzętu
- ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania;
- oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji
- karta katalogowa oferowanego sprzętu w języku polskim

II.I.GOPS.2 Zasilacz awaryjny UPS 1200VA

parametr	charakterystyka [wymagania minimalne]
moc pozorna	min. 1200VA
moc rzeczywista	min. 780W
Typ obudowy	wolnostojąca
Napięcie wejściowe	~160V – 264V ± 2%
Częstotliwość napięcia wejściowego	45 - 55Hz ± 1Hz
Zakres napięcia wyjściowego	~184V – 264V ± 2%
Kształt napięcia wyjściowego	taki jak na wejściu
Progi przetwarzania sieć – UPS	~160V / 264V ± 2%
Czas przetwarzania sieć – UPS	<3ms
Napięcie wyjściowe	~230V ± 5%
Częstotliwość napięcia wyjściowego	50Hz ± 1Hz
Kształt napięcia wyjściowego na pracy baterijnej	sinus
Progi przetwarzania UPS – sieć	~165V / 259V ± 2%
Zabezpieczenie przeciwzwarciowe	elektroniczne
Zabezpieczenie przeciążeniowe	elektroniczne
Czas podtrzymania (P1,0/0,8max/P0,5max)	minimum 3/4/8 min
akumulatory wewnętrzne	minimum 2szt 12V7Ah; szczelne, bezobsługowe
wejście zasilania	przewód podłączony na stałe do UPS'a zakończony wtyczką unischuko
Ilość i typ gniazd wyjściowych	2 standardu polskiego określone w normach PN-E-93201:1997 i PN-IEC 60884:2006
Sygnalizacja	diodowa, wskazująca pracę sieciową, baterijną, przeciążenie i ładowanie akumulatora
Interfejs komunikacyjny oprogramowanie	USB (kabel w komplecie) oprogramowanie do zarządzania i monitorowania pracy UPS w języku polskim
Gwarancja oraz serwis	minimum 36 miesięcy na elektronikę i 24 miesiące na akumulatory; autoryzowany serwis producenta zlokalizowany w Polsce. serwis realizowany w systemie door to door
Certyfikaty, oświadczenia (należy dołączyć do oferty)	- deklaracja CE producenta sprzętu - ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania; - oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji

- karta katalogowa oferowanego sprzętu w języku polskim

REALIZACJA W RAMACH ETAPU II

URZĄD GMINY W WIELKIEJ NIESZAWCE [UG]

II.II.UG.1 Zasilacz awaryjny – UPS 850VA

<i>parametr</i>	<i>charakterystyka [wymagania minimalne]</i>
moc pozorna	min. 850VA
moc rzeczywista	min. 480W
Typ obudowy	wolnostojąca
Napięcie wejściowe	$\sim 170 \div 280 \text{ V AC} \pm 7 \%$
Częstotliwość napięcia wejściowego	$45 - 55 \text{ Hz} \pm 1 \text{ Hz}$
Zakres napięcia wyjściowego	$230 \text{ V AC} \pm 10 \%$
Progi przelączania sieć – UPS	$\sim 170 \div 280 \text{ V AC} \pm 7 \%$
Czas przelączania sieć – UPS	<6ms
Napięcie wyjściowe	$\sim 230 \text{ V} \pm 5\%$
Częstotliwość napięcia wyjściowego	$50 \text{ Hz} \pm 1 \text{ Hz}$
Kształt napięcia wyjściowego na pracy rezerwowej	Schodkowa aproksymacja sinusoidy
Progi przelączania UPS – sieć	$\sim 176 \text{ V} \div 274 \text{ V AC} \pm 7 \%$
Zabezpieczenie przeciwzwarcowe	elektroniczne
Zabezpieczenie przeciążeniowe	elektroniczne
Czas podtrzymania (P1,0/0,8max/P0,5max)	minimum 2/6 min
akumulatory wewnętrzne	minimum 1 szt 12V9Ah; szczelne, bezobsługowe
Ilość i typ gniazd wyjściowych	minimum 2 standardu polskiego określone w normach PN-E-93201:1997 i PN-IEC 60884:2006
Sygnalizacja	diodowa, wskazująca pracę sieciową, baterijną, przeciążenie i ładowanie akumulatora
oprogramowanie	wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, wymagane wsparcie producenta w języku polskim odnośnie konfiguracji i rozwiązywania problemów. oprogramowanie do zarządzania i monitorowania pracy UPS w języku polskim, do pobrania ze strony producenta
Gwarancja oraz serwis	minimum 36 miesięcy na elektronikę i 24 miesiące na akumulatory; autoryzowany serwis producenta zlokalizowany w Polsce. serwis realizowany w systemie door to door
Certyfikaty, oświadczenia (należy dołączyć do oferty)	- deklaracja CE producenta sprzętu - ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania; - oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji - karta katalogowa oferowanego sprzętu w języku polskim

II.II.UG.2 Zasilacz awaryjny – UPS 1600VA

<i>parametr</i>	<i>charakterystyka [wymagania minimalne]</i>
moc pozorna	min. 1600VA
moc rzeczywista	min. 1040W
Typ obudowy	wolnostojąca
Napięcie wejściowe	~160V – 264V ± 2%
Częstotliwość napięcia wejściowego	45 - 55Hz ± 1Hz
Zakres napięcia wyjściowego	~184V – 264V ± 2%
Kształt napięcia wyjściowego	taki jak na wejściu
Progi przetaczania sieć – UPS	~160V / 264V ± 2%
Czas przetaczania sieć – UPS	<3ms
Napięcie wyjściowe	~230V ± 5%
Częstotliwość napięcia wyjściowego	50Hz ± 1Hz
Kształt napięcia wyjściowego na pracy bateryjnej	sinus
Progi przetaczania UPS – sieć	~165V / 259V ± 2%
Zabezpieczenie przeciwzwarciowe	elektroniczne
Zabezpieczenie przeciążeniowe	elektroniczne
Czas podtrzymania (P1,0/0,8max/P0,5max)	minimum 4/5/8 min
akumulatory wewnętrzne	minimum 3szt 12V5Ah; szczelne, bezobsługowe
wejscie zasilania	przewód podłączony na stałe do UPS'a zakończony wtyczką unischuko
Ilość i typ gniazd wyjściowych	2 standardu polskiego określone w normach PN-E-93201:1997 i PN-IEC 60884:2006
Sygnalizacja	diodowa, wskazująca pracę sieciową, baterijną, przeciążenie i ładowanie akumulatora
Interfejs komunikacyjny	USB (kabel w komplecie)
oprogramowanie	oprogramowanie do zarządzania i monitorowania pracy UPS w języku polskim
Gwarancja oraz serwis	minimum 36 miesięcy na elektronikę i 24 miesiące na akumulatory; autoryzowany serwis producenta zlokalizowany w Polsce. serwis realizowany w systemie door to door
Certyfikaty, oświadczenia (należy dołączyć do oferty)	- deklaracja CE producenta sprzętu - ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania; - oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji - karta katalogowa oferowanego sprzętu w języku polskim

CZĘŚĆ III

REALIZACJA W RAMACH ETAPU I

GMINNY OŚRODEK POMOCY SPOŁECZNEJ

III.I.GOPS.1 Serwer 1

<i>parametr</i>	<i>charakterystyka [wymagania minimalne]</i>
Obudowa	Obudowa Tower z możliwością instalacji 4 dysków 3,5"
Płyta główna	Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych
Procesor	Jeden procesor 6-rdzeniowy, min. 2.6GHz, umożliwiający osiągnięcie wyniku min. 40 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org w konfiguracji jednoprocessorowej.
Pamięć RAM	1x32GB pamięci RAM ECC UDIMM o częstotliwości pracy 3200MT/s.
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Wbudowane porty	min. 5 porty USB w tym 1 port USB 3.0 z tyłu obudowy, 1 port VGA na tylnym panelu, min. 1 port RS232
Gniazda PCI	Min. 2 sloty PCIe generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.
Kontroler RAID	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10..
Dyski twarde	Zainstalowane 2 dyski HDD SATA o pojemności min. 4TB, 6Gbps 7.2K oraz 2 dyski SSD SATA o pojemność dysku minimum 960 GB, Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
System operacyjny/System wirtualizacji	Windows Server 2022 Essentials 10 RDZENI lub równoważny Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez

- konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
 - a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - c. umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów,
 - d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
 13. Możliwość dystrybucji ruchu sieciowego http pomiędzy kilka serwerów.
 14. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
 - a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
 - b. Dotykowy umożliwiający sterowanie dotykem na monitorach dotykowych.
 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
 18. Mechanizmy logowania w oparciu o:
 - a. Login i hasło,

- b. Karty z certyfikatami (smartcard),
 - c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
- a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 - b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
 - Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows
 - c. Zdalna dystrybucja oprogramowania na stacje robocze.

- d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
 - e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - Dystrybucję certyfikatów poprzez http
 - Konsolidację CA dla wielu lasów domeny,
 - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
 - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
 - f. Szyfrowanie plików i folderów.
 - g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
 - h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
 - i. Serwis udostępniania stron WWW.
 - j. Wsparcie dla protokołu IP w wersji 6 (IPv6),
 - k. Wsparcie dla algorytmów Suite B (RFC 4869),
 - l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
 - m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
 - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
 - Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 - Obsługi 4-KB sektorów dysków
 - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
 - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
 - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. Trunk mode)
26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego

Zasilacze**Karta Zarządzania**

rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

Jeden zasilacz o mocy min. 300W. Wraz z kablami zasilającymi.

Niezależna od zainstalowanego na serwerze systemu operacyjnego, karta zarządzająca, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:

- **Interfejsy użytkownika:** HTML5 Web UI, Redfish, WS-Man, IPMI 2.0, DCMI 1.5, RACADM, SMASH-CLP, Telnet, SSH, Przekierowanie szeregowo
- **Łączność:** Współużytkowana karta LOM, oddzielna karta sieciowa (NIC), VLAN, IPv4/6, DHCP, statyczny adres IP, dynamiczny DNS, iDRAC Direct (port USB), widok połączeń, NFS v4, NTLMv1/2
- **Bezpieczeństwo:** Silikonowy element zaufania w kontrolerze iDRAC i przy rozruchu, podpisane aktualizacje oprogramowania wewnętrznego, RBAC, użytkownicy lokalni, szyfrowanie SSL/TLS, FIPS, certyfikaty UEFI, zabezpieczone domyślne hasło (losowo), niestandardowy baner logowania do zabezpieczeń
- **Obecność zdalna:** sterowanie zasilaniem, sterowanie rozruchem, szeregowo przez LAN (SOL)
- **Zasilanie i temperatura:** miernik energii działający w czasie rzeczywistym, monitorowanie temperatury, dostosowana temperatura na wylocie
- **Monitorowanie stanu:** pełny monitoring bez agentów, przewidywanie awarii (w tym inteligentne powiadomienia do dysków), SNMPv1/2/3, wentylatory, zasilacz, pamięć, procesor, RAID, karta interfejsu sieciowego, obudowy do pamięci masowych z możliwością bezpośredniego podłączania, poziomy zużycia dysku SSD
- **Aktualizacja oprogramowania wewnętrznego:** Zdalne aktualizacje bez użycia agentów, wbudowane narzędzia do aktualizacji (interfejs użytkownika F10/iDRAC)
- **Wdrożenie:** Konfiguracja lokalna przy użyciu interfejsu użytkownika F10 LC, zdalne wdrażanie systemu operacyjnego, strony konfiguracji systemu BIOS i RAID, zdalna konfiguracja serwera, importowanie i eksportowanie profilu konfiguracji serwera (SCP), pakiet sterowników systemu operacyjnego, spis systemu, wymazywanie systemu w celu wycofania serwera lub zmiany jego wykorzystania.
- **Diagnostyka, serwis i rejestrowanie:** Dzienniki dziennika SEL i kontrolera cyklu eksploatacji, narzędzia diagnostyczne, przywracanie konfiguracji serwera, łatwe przywracanie po

Certyfikaty

wymianie płyty głównej, diody LED stanu, opcjonalny wyświetlacz LCD na ramce, port serwisowy iDRAC Direct, zdalny i lokalny reset kontrolera iDRAC, wirtualny NMI, watchdog systemu operacyjnego, raport z kolekcji SupportAssist, bezpośrednia rejestracja SupportAssist, uwagi robocze, zarządzanie licencjami

- **Udoskonalenia interfejsu użytkownika:** Nowe pole wyszukiwania ułatwiające nawigację, przegląd kolejki zadań, zwinięty styl harmonijki dla szybszego ładowania stron, wyświetlanie kolekcji SupportAssist w interfejsie użytkownika

Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001

Serwer musi posiadać deklarację 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

Gwarancji producenta: 5 lat

Możliwość rozszerzenia gwarancji przez producenta do 7 lat.

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.

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)

Warunki gwarancji**III.I.GOPS.2 Serwer 2**

parametr
Obudowa

charakterystyka [wymagania minimalne]

Obudowa Tower z możliwością instalacji 4 dysków 3,5"

Płyta główna**Chipset****Procesor****Pamięć RAM****Karta graficzna****Wbudowane porty****Gniazda PCI****Interfejsy sieciowe/FC/SAS****Kontroler RAID****Dyski twarde****Zasilacze****Karta Zarządzania**

Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych

Jeden procesor 6-rdzeniowy, min. 2.6GHz, umożliwiający osiągnięcie wyniku min. 40 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org w konfiguracji jednoprocessorowej.

1x32GB pamięci RAM ECC UDIMM o częstotliwości pracy 3200MT/s. Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200

min. 5 porty USB w tym 1 port USB 3.0 z tyłu obudowy, 1 port VGA na tylnym panelu, min. 1 port RS232

Min. 2 sloty PCIe generacji 4

Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.

Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10..

Zainstalowane 2 dyski HDD SATA o pojemności min. 4TB, 6Gbps 7.2K oraz 2 dyski SSD SATA o pojemność dysku minimum 960 GB, Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.

Jeden zasilacz o mocy min. 300W. Wraz z kablami zasilającymi.

Niezależna od zainstalowanego na serwerze systemu operacyjnego, karta zarządzająca, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:

- **Interfejsy użytkownika:** HTML5 Web UI, Redfish, WS-Man, IPMI 2.0, DCMI 1.5, RACADM, SMASH-CLP, Telnet, SSH, Przekierowanie szeregowo
- **Łączność:** Współużytkowana karta LOM, oddzielna karta sieciowa (NIC), VLAN, IPv4/6, DHCP, statyczny adres IP, dynamiczny DNS, iDRAC Direct (port USB), widok połączeń, NFS v4, NTLMv1/2
- **Bezpieczeństwo:** Silikonowy element zaufania w kontrolerze iDRAC i przy rozruchu, podpisane aktualizacje oprogramowania wewnętrznego, RBAC, użytkownicy lokalni, szyfrowanie SSL/TLS, FIPS, certyfikaty UEFI, zabezpieczone domyślne hasło (losowo), niestandardowy baner logowania do zabezpieczeń
- **Obecność zdalna:** sterowanie zasilaniem, sterowanie rozruchem, szeregowo przez LAN (SOL)
- **Zasilanie i temperatura:** miernik energii działający w czasie rzeczywistym, monitorowanie temperatury, dostosowana temperatura na wylocie
- **Monitorowanie stanu:** pełny monitoring bez agentów, przewidywanie awarii (w tym inteligentne powiadomienia do dysków), SNMPv1/2/3, wentylatory, zasilacz, pamięć, procesor, RAID, karta interfejsu sieciowego, obudowy do pamięci masowych z możliwością bezpośredniego podłączania, poziomy zużycia dysku SSD

- **Aktualizacja oprogramowania wewnętrznego:** Zdalne aktualizacje bez użycia agentów, wbudowane narzędzia do aktualizacji (interfejs użytkownika F10/iDRAC)
- **Wdrożenie:** Konfiguracja lokalna przy użyciu interfejsu użytkownika F10 LC, zdalne wdrażanie systemu operacyjnego, strony konfiguracji systemu BIOS i RAID, zdalna konfiguracja serwera, importowanie i eksportowanie profilu konfiguracji serwera (SCP), pakiet sterowników systemu operacyjnego, spis systemu, wymazywanie systemu w celu wycofania serwera lub zmiany jego wykorzystania.
- **Diagnostyka, serwis i rejestrowanie:** Dzienniki dziennika SEL i kontrolera cyklu eksploatacji, narzędzia diagnostyczne, przywracanie konfiguracji serwera, łatwe przywracanie po wymianie płyty głównej, diody LED stanu, opcjonalny wyświetlacz LCD na ramce, port serwisowy iDRAC Direct, zdalny i lokalny reset kontrolera iDRAC, wirtualny NMI, watchdog systemu operacyjnego, raport z kolekcji SupportAssist, bezpośrednia rejestracja SupportAssist, uwagi robocze, zarządzanie licencjami
- **Udoskonalenia interfejsu użytkownika:** Nowe pole wyszukiwania ułatwiające nawigację, przegląd kolejki zadań, zwinięty styl harmonijki dla szybszego ładowania stron, wyświetlanie kolekcji SupportAssist w interfejsie użytkownika

Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001

Serwer musi posiadać deklarację 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

Gwarancji producenta: 5 lat

Możliwość rozszerzenia gwarancji przez producenta do 7 lat.

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.

Możliwość rozszerzenia gwarancji o:

Wyznaczonego przez wykonawcę Opiekuna Technicznego Klienta, do którego obowiązków będzie należało:

Monitorowanie zdarzeń w obrębie infrastruktury

Certyfikaty

Warunki gwarancji

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)

III.1. GOPS.3 Oprogramowanie oraz monitoring usług i użytkowanych systemów

Przez wdrożenie systemu monitorowania Zamawiający rozumie dostawę licencji, zaprojektowanie systemu oraz jego uruchomienie, a także przeprowadzenie instruktażu z zakresu administracji i jego obsługi.

System monitorowania ma stanowić narzędzie pozwalające na gromadzenie i analizowanie danych dotyczących różnorodnych zdarzeń związanych z użytkowaniem przez Zamawiającego systemami teleinformatycznymi wraz z powiadamianiem zespołów bezpieczeństwa.

Zaproponowane rozwiązanie powinno wspierać zespół monitorowania w procesie reakcji na wykryte incydenty. System ma przetwarzać dane zarówno w celu bezpośredniego monitorowania systemów i usług jak i także w celu wsparcia procesu utrzymywania zgodności z regulacjami prawnymi oraz standardami bezpieczeństwa, w szczególności w celu wypełnienia obowiązków wynikających z:

- Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,
- Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych,
- Ustawy z dnia 10 listopada 2020 r. o doręczeniach elektronicznych
- Rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej,
- Ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
- Ustawy z dnia 5 września 2016 r. o usługach zaufania i identyfikacji elektronicznej,
- Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną,
- Ustawę z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach,
- Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych.

parametr

charakterystyka [wymagania minimalne]

Wykrywanie i monitorowanie

Monitorowanie infrastruktury IT, w tym serwerów i usług.
 System pozwala na monitorowanie zdefiniowanych zdarzeń, w tym zbieranie, analizowanie i wizualizację danych.
 System jest przystosowany do przetwarzania danych typowych dla systemów teleinformatycznych:

- Adresy IP4 i IP6
- Nazwy DNS
- Identyfikatory protokołów sieciowych np. SNMP, SSH, TELNET, IPMI, JPM, HTTP/HTTPS, VMWare
- Porty
- Nazwy i identyfikatory użytkowników
- Nazwy i identyfikatory procesów
- Nazwy i identyfikatory zasobów
- Czasu
- i innych

Interfejs i prezentacja danych

Zarządzanie monitorowanymi zasobami

System umożliwia wykrywanie wszelkich problemów w infrastrukturze Zamawiającego i powiadamia wskazanych użytkowników

System zapewnia graficzny interfejs użytkownika dostępny wyłącznie za pomocą przeglądarki internetowej.

System wspiera generowanie mapy monitorowane środowiska uwzględniającej prezentację co najmniej urządzeń, portów, prędkości połączeń i nazw urządzeń.

System prezentuje dane na wykresach w czasie rzeczywistym.

System pozwala na tworzenie własnych wykresów gromadzących i prezentujących wiele danych.

Interfejs użytkownika wyodrębnia prezentację co najmniej następujących danych:

- problemy
- hosty
- mapy
- usługi
- SLA
- Zasoby
- Raporty
- Kolekcje danych
- Alerty
- Administracja i zarządzanie, w tym zarządzanie użytkownikami.

System musi udostępniać ogólnodostępną wyszukiwarkę, która w łatwy sposób pozwala odnaleźć hosty, grupy i schematy.

System pozwala na tworzenie własnych motywów interfejsu użytkownika.

System pozwala na rebranding obejmujących co najmniej możliwość wstawienia własnego loga.

System pozwala na zarządzanie użytkownikami korzystającymi z interfejsu przeglądarkowego.

Użytkownicy mogą pełnić różne role w systemie oraz należeć do wielu grup użytkowników.

Uprawnienia w systemie muszą pozwalać na przydzielenie dostępu do:

- dashboardu
- monitoringu procesów, hostów, mapy
- usług i weryfikacji poziomu SLA
- zasobów w tym serwerów
- raportów i notyfikacji
- kolekcji gromadzonych danych
- alertów
- API

System umożliwia zarządzania hostami, w tym przydzielanie ich do grup i stosowanie dla nich wbudowanych standardowych schematów (templates) monitorowania.

System pozwala na definiowanie i zarządzanie monitorowanymi parametrami.

System oferuje minimum 50 monitorowanych parametrów obejmujących co najmniej następujące grupy/typy:

- Jądro systemu (kernel)
- Monitorowanie logów
- Parametry dotyczące sieci
- Procesy
- Czujniki sprzętowe
- Parametry systemu
- System plików
- Pamięć
- Strony internetowe

Raportowanie i
alarmowanie
licencjonowanie

System pozwala na tworzenie własnych skryptów oraz definiowanych własnych triggerów wyzwalających zdarzenie za pomocą obsługiwanych przez system wyrażeń regularnych.

Wyrażenia muszą obsługiwać funkcje, ich parametry i operatory. Liczba oferowanych funkcji – min. 50 i operatorów – min. 10.

System musi posiadać możliwość tworzenia własnych schematów monitorowania.

System musi pozwalać na definiowanie pożądanych parametrów SLA.

System musi posiadać wbudowane narzędzia monitorowania środowiska VMware

System pozwala na przysyłanie notyfikacji/powiadomień dla zdefiniowanych zdarzeń poprzez email z wykorzystaniem serwera/ usługi Zamawiającego

Zamawiający wymaga dostarczenia licencji wieczystej z prawem do aktualizacji. Licencja na System nie może narzucać jakichkolwiek dodatkowych wymagań dla Zamawiającego skutkujących ponoszeniem dodatkowych kosztów związanych z jej utrzymaniem.

Licencja musi obejmować wszystkie funkcjonalności zaoferowanego oprogramowania i pozwalać na monitorowanie dowolnej liczby urządzeń infrastruktury, serwerów i usług IT.

Licencja nie może w żaden sposób być przypisana do użytkownika, serwera czy maszyny. Nie może być także uzależniona od liczby rdzeni procesora.

Licencja musi pozwalać na zainstalowanie oprogramowania w dowolnej liczbie instancji – ma być licencją udzieloną na Zamawiającego, bez ograniczania liczby instalacji oprogramowania.

Wsparcie techniczne

Gwarancja producenta i wsparcie techniczne - nie później niż do 30.06.2026r. obejmująca:

dostarczanie aktualizacji Systemu, udzielanie konsultacji telefonicznych / mailowych w zakresie funkcjonowania i konfiguracji Systemu oraz jego rozszerzania

Minimalny zakres
monitorowanych
systemów i usług - źródła
danych

W ramach wdrożenia Systemu monitorowaniem objęte zostaną następujące źródła zdarzeń:

Serwery i aplikacje kluczowych baz danych – 1 szt.

Serwer WWW – 1 szt. (www/bip)

Urządzenie brzegowe – 1 szt.

Serwer poczty elektronicznej 1 szt.

Switch (SNMP) – min. 1 szt.

Monitorowanie integracji z systemem ePUAP – 1 szt.

Monitorowanie integracji z systemem eDoręczeń – 1 szt.

Sumarycznie przewiduje się podłączenie nie więcej niż 7 źródeł danych rozumianych jako serwer/urządzenie sieciowe, generujących różne rodzaje zdarzeń w liczbie szacunkowo kilku tysięcy na dobę.

Zakres prac i wdrożenia

1. Zebranie informacji dotyczących monitorowanej infrastruktury, monitorowanych źródeł danych.
2. Instalację i konfigurację systemu w zasobach informatycznych Zamawiającego – preferowane środowisko Linux
3. Uzgodnienie i wdrożenie sposobu backupu Systemu.
4. Dostarczenie licencji na System.
5. Uzgodnienie mechanizmów funkcjonalnych z Zamawiających oraz ich wdrożenie.
6. Przeprowadzenie instruktażu/warsztatu szkoleniowego w wymiarze 2h
7. Skonfigurowanie i uruchomienie mechanizmów powiadomień o zdarzeniach krytycznych.

ETAP II

URZĄD GMINY W WIELKIEJ NIESZAWCE

III.II.UG.1 System umożliwiający monitoring komputerów

System musi umożliwić bezproblemową i stabilną obsługę co najmniej 50 Klientów jednocześnie, musi posiadać co najmniej 1 dostęp administracyjny

parametr

charakterystyka [wymagania minimalne]

Architektura / budowa

1. **Błąd! Nie można odnaleźć źródła odwołania.:**

1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przysyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.

- Połączenie klient – serwer, Komunikacja odbywa się z wykorzystaniem TLS 1.3.

- Serwer i klient posiadają certyfikaty SSL (4096 bitowe).

2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych).

3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników i uruchamiana na komputerach pracowników udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach zgodnie ze specyfikacją opisaną poniżej.

4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.

5. Baza danych powinna umożliwiać pracę na silniku Microsoft SQL w wersji bezpłatnej lub komercyjnej.

2. Konfiguracja Architektury:

1. Komponenty Klient, konsola administracyjna, serwer, baza danych muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerów aktualizacji producenta systemu.

2. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja Klientów musi przebiegać w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie od producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją.

3. System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, pakietów, pomoc i inne wbudowane bazy wiedzy.

4. Klient do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI.

5. Klient musi być dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku *.msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku *.msi.

Wymagania systemowe

Interfejsy

6. Klient musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej.
 7. System zapewnia możliwość stworzenia instalatora (.exe) z wbudowanymi, zaszyfrowanymi poświadczeniami dla dowolnego konta. Funkcja ta umożliwia instalację usługi bezpośrednio na kontach użytkowników – zarówno lokalnych, jak i domenowych, korzystając z uprawnień zdefiniowanych dla instalatora w konsoli systemu.
 8. Klient musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa).
 9. System powinien umożliwiać generowanie unikatowego identyfikatora Klienta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków.
 10. Klient musi mieć definiowalny priorytet pracy (ABOVE_NORMAL, NORMAL, BELOW_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów.
 11. Klient musi wspierać wiele różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu Klienta.
 12. System musi umożliwiać komunikację pomiędzy Klientami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.
 13. System musi mieć możliwość współpracy komponentów Klient i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami Klientów. System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem.
 14. Automaty powinny realizować co najmniej:
 - Usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nie przyrostowe, zmniejszanie bazy danych).
 15. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartości parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie
-
1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera).
 2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.
 - 2.1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2
 3. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11.
 4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 8+).
 5. Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych komercyjnych lub bezpłatnej - Microsoft SQL Server Express Edition.
 6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare
 1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.

Funkcjonalności systemu zarządzania infrastrukturą IT

- 1.1. Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.
- 1.2. Import z Active Directory musi wspierać obsługę protokołów SSL oraz TLS.
- 1.3. Import z Active Directory musi umożliwiać podanie więcej niż jednej domeny.
2. System musi umożliwiać import użytkowników z zewnętrznego pliku CSV.
3. System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switchy itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, dacie zakupu, gwarancji. Interfejs dodatkowo musi umożliwiać importowanie użytkowników, struktur i licencji. Import musi umożliwiać pobieranie danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku *.xls, pliku *.xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane.
4. System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS.
5. System zapewnia integrację z modelem LLM
1. Funkcjonalność Klienta
 - 1) System musi umożliwiać pełne zdalne zarządzanie Klientami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączenia Klienta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego).
 - 2) Klient musi mieć możliwość konfiguracji zakresu skanowania plików w oparciu o nazwę plików (z uwzględnieniem znaków wieloznacznych), lokalizację na konkretnym dysku, datę utworzenia pliku oraz wielkość
 - 3) Klient musi mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej, konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkownika, który go wyświetlił.
2. Funkcjonalność konsoli administracyjnej.
 - 1) Konsola musi być w pełni polskojęzyczna oraz dodatkowo posiadać wersję językową angielską.
 - 2) Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie).
 - 3) Konsola administracyjna musi posiadać minimum 140 dashboardów – dashboard użytkownika, dashboard prezentujący parametry infrastruktury, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie.
 - 4) Dashboard użytkownika jest budowany samodzielnie przez użytkownika poprzez wybór szybkiego skrótu do dowolnego ekranu aplikacji lub wybór widżetu.
 - 5) Dashboard prezentujący parametry sieci zawiera widżety pogrupowane w kategorie: Czat, Gry, Peer to peer, Streaming, Usługa podstawowa, Usługa podstawowa (szyfrowana), Złośliwe oprogramowanie.
 - 6) Dla każdej z usług prezentowane są relacje do wszystkich komputerów zawierające połączenia: powolne, nieosiągalne, rozłączone i poprawne wraz z czasami połączeń.
 - 7) Dashboard prezentujący informacje o bezpieczeństwie zawiera widżety zawierające informacje: błędy serwera zadań, błędy smart, komputery bez BitLockera, komputery bez połączenia z serwerem, komputery z błędami typu critical / error / warning, duży transfer sieciowy, komputery bez Klienta, komputery offline, komputery online, komputery z naruszoną polityką dlp, komputery z nieaktualną polityką dlp, liczba administratorów lokalnych w systemie (online), logowanie w godzinach nocnych, monitorowanie transferu do dysków chmurowych, nieautoryzowana pamięć usb, nowe komputery, nowe urządzenia w sieci, oprogramowanie zabronione, przekroczone cał, przekroczone licencje, subskrypcje, które wygasły, systemy bez wsparcia, wielokrotne logowanie, wysokie użycie CPU, wysokie użycie ram, zaległe szkolenia wideo, zaległe wiadomości elearning, zbyt mało miejsca na hdd, zmiany na kontach użytkowników, zmiany tcp/ip.

- 8) Konsola administracyjna musi być wyposażona w panel zawierający graficzne widżety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi.
- 9) Dane na widżetach muszą być aktualizowane automatycznie.
- 10) Widżety muszą być skojarzone dziedzinowo ze wszystkimi obszarami zarządzania infrastrukturą, a każdy obszar powinien być reprezentowany odpowiadające mu widżety (np. w obszarze zarządzania komputerami system powinien być wyposażony w widżety zawierające: ilość komputerów w ramach danego typu, ilość komputerów on/off-line, strukturę komputerów wg ilości pamięci RAM, ilość komputerów wg ilości wolnego miejsca na dysku, ilość komputerów wg dat ostatnich połączeń)
- 11) System musi posiadać filtr roboczy, przeszukujący całą tabelę po zdefiniowanym słowie.
- 12) System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widżety, ich konfigurację i kolejność).
 - a. System musi oferować możliwość dodawania własnych pól zarówno w głównym widoku, jak i w obszarze zarządzania użytkownikami. Te definiowalne pola powinny być w pełni funkcjonalne i umożliwiać:
 - i Dodawanie nazwy kolumny, określenie jej typu oraz możliwość ograniczenia liczby znaków, które można wprowadzić.
 - ii Wśród obsługiwanych typów pól znajdują się: tekst, liczba całkowita, liczba, data, data i czas, combobox.
 - b. W ramach personalizacji widoku, system powinien oferować możliwość zastosowania filtrów dostosowujących zawartość danego widoku. Filtry te powinny:
 - i Bazować na kolumnach dostępnych w danym widoku.
 - ii Umożliwiać selekcję operacji filtrujących takich jak: równość, nierówność, większość, mniejszość, obecność lub brak wartości.
 - iii Pozwalać na łączenie filtrów przy użyciu logicznych operatorów „AND” (i), „OR” (lub), „NOT AND” (i nie), „NOT OR” (lub nie).
 - iv Być zapamiętywane przez system dla konkretnej sesji użytkownika i pozostawać aktywne po ponownym zalogowaniu.
- 13) Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu. Reguły muszą być zapamiętywane i dostępne w kolejnych sesjach oraz oparte co najmniej o: nazwę komputera, IP, rodzaj systemu operacyjnego, identyfikator Klienta, strukturę organizacyjną, stan Klienta (włączony/wyłączony), nazwę użytkownika zalogowanego, producenta sprzętu, dostawcę sprzętu, lokalizację komputera, dowolnie zdefiniowaną przez użytkownika wartość (np. kolor obudowy komputera). Użytkownik może wybrać za jednym razem więcej niż jedną regułę. Zmiana wybranej reguły powoduje aktualizację wyświetlonego widoku.
- 14) Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą mieć możliwość filtrowania kolumnowego.
- 15) System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.
- 16) Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu.
- 17) Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko).

- 18) Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja Klienta, stanu Klienta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera.
- 19) Konsola musi umożliwić bezpośrednie przejście do witryny internetowej producenta z poziomu repozytorium producentów (o ile taka jest dostępna, np. DELL).
- 20) Konsola musi umożliwić bezpośrednie przejście do strony producenta zawierającej dodatkowe dane konfiguracyjne na temat konkretnego komputera w oparciu o Service Tag lub inny unikatowy identyfikator (np. Dell)
- 21) Konsola musi zawierać w sobie pełną dokumentację systemu, dokumentacja musi być na bieżąco aktualizowana poprzez automatyczne mechanizmy aktualizacji z serwera aktualizacji producenta.
3. Funkcjonalność panelu pracownika
 - 1) Automatyczne uruchamianie panelu oraz autoryzacja w momencie zalogowania użytkownika do systemu operacyjnego.
 - 2) Zakres informacji w panelu jest definiowany przez administratora w formie schematów przypisywanych dla wybranych grup pracowników.
 - 3) Panel pracownika użytkowany przez kierownika zawiera dodatkowo dane dostępne w panelach podległych pracowników w formie danych skumulowanych i analitycznych.
 - 4) Wszelkie informacje udostępniane w panelu pracownika pogrupowane są w logiczne sekcje, z możliwością indywidualnego bądź grupowego włączania / wyłączania (ukrywania) sekcji.
 - 5) Sekcje informacyjne panelu pracownika
 - a. Zalogowany użytkownik – imię i nazwisko, IP, nazwa komputera, informacje z AD – Nazwa użytkownika, Imię, Nazwisko, E-mail, Firma, Dział, Stanowisko, Struktura org., Kraj, Województwo, Miasto, Ulica, Kod pocztowy, Telefon, Telefon komórkowy, Opis, WWW, GG, Skype, Adres, Biuro, Skrytka pocztowa
 - 6) Dashboard
 - a. Mój komputer – wykorzystanie RAM, Dysk, CPU.
 - b. Produktywność - czas zalogowania, aktywność, produktywność.
 - c. Wiadomości – lista ostatnich wiadomości przestanych pracownikowi.
 - d. Skrót – definiowane przez administratora skróty do adresów URL, z możliwością edycji tytułu, opisu, koloru tekstu i tła
 - 7) Sprzęt
 - a. Komputery przypisane do pracownika (nr seryjny, MAC, IP, data ostatniego logowania).
 - b. Komputery używane przez pracownika (nr seryjny, MAC, IP, data ostatniego logowania).
 - c. Urządzenia przypisane do pracownika (nr seryjny, typ, IP).
 - 8) Oprogramowanie
 - a. Lista używanego oprogramowania (nazwa aplikacji, wersja, Producent, użycie w okresie ostatnich 3, 6, 12 miesięcy, data ostatniego uruchomienia).
 - 9) Informacja o czasie pracy
 - a. Lista otwartych sesji pracownika lub grupy pracowników (data zalogowania, nazwa komputera, IP, rodzaj połączenia (LAN, NAT, VPN), czas zalogowania).
 - b. Lista ostatnich sesji użytkownika lub grupy użytkowników (początek, koniec, czas trwania sesji, nazwa komputera, IP)
 - c. Lista używanego oprogramowania (nazwa aplikacji, wersja, producent, data ostatniego uruchomienia, użycie aplikacji w ostatnich 3, 6, 12 miesiącach).
 - d. Aktywność użytkownika lub użytkowników w aplikacjach (aplikacja, kategoria aplikacji, łączny czas korzystania, czas korzystania aktywnego, czas korzystania pasywnego).
 - e. Aktywność użytkownika lub użytkowników w Internecie (adres URL, informacja o stronie www – kategoria strony czy strona jest produktywna, łączny czas korzystania, czas aktywności, czas pasywności).
 - f. Wydruki – lista wydrukowanych dokumentów – data, godzina, nazwa drukarki, nazwa dokumentu
4. Zarządzanie licencjami

- 1) System musi umożliwiać zarządzanie licencjami w ramach dowolnego elementu struktury organizacyjnej (dla wybranej struktury organizacyjnej pokazuje liczbę instalacji i liczbę licencji w danym modelu licencjonowania wraz z listą komputerów).
- 2) System musi dawać możliwość wykonywania (historia) wielu audytów legalności i zapamiętywać wyniki tych audytów w odniesieniu do systemów operacyjnych jak i aplikacji/pakietów, z uwzględnieniem segmentu struktury organizacyjnej.
- 3) Zarządzanie oprogramowaniem musi następować z podziałem na aplikacje i pakiety oprogramowania.
- 4) System musi pozwalać na zdefiniowanie dowolnej ilości tzw. „standardów oprogramowania”, które definiują 3 kategorie oprogramowania: „oprogramowanie zalecane” – pozycje z tej listy są wymagane do zainstalowania obowiązkowo na każdym komputerze, „oprogramowanie dodatkowe” – pozycje z tej listy mogą być zainstalowane (nie jest to wymagane) a instalacja odbywa się na wniosek samego użytkownika lub jego przełożonego, „oprogramowanie nieokreślone” – oprogramowanie nie należące do żadnej z dwóch powyżej zdefiniowanych kategorii a zidentyfikowane na komputerze.
- 5) System umożliwia zdefiniowanie listy aplikacji zabronionych.
- 6) System umożliwia utworzenie schematów (kolekcji) oprogramowania zabronionego i w momencie pojawienia się ich na komputerze przystępuje do automatycznego odinstalowania w trybie cichym (bez interfejsu).
- 7) System musi umożliwiać kategoryzację uruchamianych procesów.
 - a. Umożliwia zdefiniowanie dowolnej kategorii oprogramowania/pliku/procesu i samodzielnej przydzielenie oprogramowania/pliku/procesu do kategorii.
 - b. W oparciu o Machine learning system umożliwia analizę procesów oraz przypisanie im odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem uruchamianych procesów.
 - c. Automatyczne przypisanie kategorii do każdego uruchomionego procesu.
 - d. Niezależność od zewnętrznych dostawców bazy wzorców procesów.
- 8) System zbiera szczegółowe informacje o systemie operacyjnym (wersja, edycja, service pack, poprawki, data instalacji).
- 9) System umożliwia odczytywanie identyfikatorów i kluczy produktowych dla systemu operacyjnego oraz dowolnego oprogramowania, tam, gdzie jest to tylko technicznie możliwe.
- 10) System wspiera następujące typy licencji: Enterprise, Licensed concurrent, Licensed Name, Licensed per Processor, Licensed per Seat, Licensed per Server, OEM, OEM Downgrade, Open, Select, MOLP Open Value (Company wide), MOLP Open Value (non-Company wide), MOLP Open Value Subscription, CAL, SAAS, Trial, Shareware, Cal Per User.
- 11) System automatycznie klasyfikuje i rozlicza licencje OEM dla systemów operacyjnych oraz licencje typu freeware dla aplikacji.
- 12) System musi pomijać w rozliczeniu licencje wygasłe (po terminie ważności) i informować administratora o wygasaniu licencji.
- 13) System musi umożliwiać wyróżnianie licencji zabezpieczonych kluczami sprzętowymi.
- 14) System automatycznie wskazuje liczbę posiadanych licencji oraz liczbę używanego oprogramowania (pokazuje braki oraz nadwyżki).
- 15) System automatycznie uwzględnia i rozlicza licencje typu Upgrade i Downgrade wg zdefiniowanych przez użytkownika reguł.
- 16) System umożliwia ewidencję licencji (data zakupu, cena, dostawca, nr faktury, typ licencji, klucz produktowy, identyfikator produktowy, data wygaśnięcia, nr dokumentu OT, nr zapotrzebowania) poprzez rejestrację dokumentów źródłowych (faktur zakupu) z możliwością dołączenia dowolnych załączników z repozytorium.
- 17) System umożliwia przypisanie licencji do użytkownika i/lub komputera oraz udostępnia informację o licencjach zarejestrowanych i jednocześnie wolnych (nieprzypisanych).
- 18) System umożliwia zbieranie informacji na temat uruchamianych aplikacji na inwentaryzowanych komputerach (m.in. czas uruchomienia, nazwa zalogowanego użytkownika, nazwa aplikacji). System musi posiadać mechanizm zabezpieczający przed powstaniem niekompletnych lub niewłaściwych zapisów w wyniku braku zasilania lub innych awarii inwentaryzowanego systemu/sprzętu).

- 19) System musi udostępniać informację o uruchamianych aplikacjach w okresie 3/6/12 miesięcy oraz udostępniać datę ostatniego uruchomienia.
 - 20) System musi umożliwiać podgląd historii zmian aplikacji i pakietów na komputerach.
 - 21) System musi umożliwiać zdalne odinstalowanie oprogramowania na jednym bądź wybranych komputerach.
 - 22) System musi udostępniać informacje o stopniu wykorzystania aplikacji / pakietów dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie. W/w informacja winna być przedstawiona również w postaci graficznej.
 - 23) System musi udostępniać informacje o stopniu wykorzystania oprogramowania typu web dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie. W/w informacja winna być przedstawiona również w postaci graficznej.
5. Wzorce aplikacji i pakietów
- 1) System ma posiadać wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 4 tys. wzorców aplikacji, 1,3 tys. Producentów.
 - 2) System musi udostępniać informacje dotyczące plików, na podstawie których zidentyfikowana została dana aplikacja.
 - 3) System musi prezentować informacje o ilości i dacie publikacji posiadanej bazy wzorców oprogramowania.
 - 4) System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania.
 - 5) Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów.
 - 6) System musi mieć możliwość zamawiania bezpośrednio z poziomu konsoli administracyjnej u producenta systemu wzorców oprogramowania z możliwością wskazania dla jakiego komputera / komputerów wzorce mają być utworzone. Zamówione i utworzone przez Producenta wzorce muszą automatycznie (bez ingerencji administratora systemu) zostać zaimportowane do systemu.
 - 7) System musi rozpoznawać wersję i edycję zainstalowanych pakietów Microsoft Office (tam, gdzie jest to technicznie możliwe (np. Microsoft Office 2007 Professional, Microsoft Office 2007 Standard, Microsoft Office 2003 Standard itd.).
6. Inwentaryzacja sprzętu komputerowego
- 1) System musi umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem).
 - 2) System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language.
 - 3) System ma umożliwiać skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu).
 - 4) System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania.
 - 5) System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza poczynawszy od wskazanego miejsca w hierarchii kluczy rejestru.
 - 6) System ma umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu).
 - 7) System ma umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART).

- 8) System musi umożliwić budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku.
- 9) System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu.
- 10) System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent).
- 11) System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne).
- 12) System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów.
- 13) System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik)
- 14) System umożliwia dodawanie notatek do każdej pozycji sprzętu.
- 15) System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części).
 - a. System musi umożliwiać definiowanie typów serwisów
 - b. System musi umożliwiać definiowanie wartości serwisu
 - c. System musi umożliwiać definiowanie daty ważności serwisu oraz daty gwarancji
- 16) System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium.
- 17) System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkownika, likwidacja).
7. Inwentaryzacja urządzeń podłączanych do komputera.
 - 1) System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.)
 - 2) System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika.
 - 3) System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika).
8. Inwentaryzacja urządzeń sieciowych.
 - 1) System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNMP. Skaner musi wykryć typ urządzenia na danym IP/portcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis). Skaner musi obsługiwać SNMP w wersji 1/2c/3.
 - 2) Skaner SNMP musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.
 - 3) System musi zbierać informacje o jakości połączenia:
 - 4) Czas odpowiedzi serwisów (usług) podawany w milisekundach:
 - a. Średni czas odpowiedzi.
 - b. Minimalny czas odpowiedzi.
 - c. Maksymalny czas odpowiedzi.
 - 5) Ilość dostarczonych informacji – pakietów dostarczonych, straconych oraz procent strat.
 - 6) System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają Klienta.
 - a. Posiada niezwłoczną i automatyczną identyfikację podłączonych urządzeń do sieci
 - b. Baza wzorców musi zawierać ponad 100 monitorowanych portów i usług.
 - c. System musi umożliwiać administratorowi definiowanie dodatkowych portów do monitorowania i przypisywanie do nich usług, a także modyfikowanie istniejących rekordów, obejmujących: port TCP, kategorię, nazwę usługi oraz nazwę skróconą.
 - 7) System musi posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci.
 - a. System musi umożliwiać generowanie map według dowolnych filtrów użytkownika.

9. Inwentaryzacja sprzętu.

- 1) System musi umożliwiać inwentaryzację manualną (ewidencję) sprzętu innego niż komputery: np. drukarki, switchy, routery, monitory, pamięci masowe itp.
 - a. System musi umożliwiać bazy typów urządzeń, o dowolne typy.
- 2) System umożliwia wprowadzanie dowolnych notatek oraz zdarzeń serwisowych.
- 3) System musi monitorować zmiany ewidencyjne i ruchy sprzętu.
- 4) System musi umożliwiać przypisanie urządzenia do użytkownika, ewidencję napraw, gwarancji.
- 5) System musi mieć możliwość przypominania o upływającym terminie gwarancji.
- 6) System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium wewnętrznego systemu.
- 7) System udostępnia informację o wartości wprowadzonego sprzętu.
- 8) System musi umożliwiać samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów oraz zapewniać automatyczną numerację tych dokumentów zapewniającą unikatowość.
- 9) System musi pozwalać na kopiowanie (duplikację) dowolnego urządzenia dowolną ilość razy.
- 10) System musi pozwalać na ewidencję umów utrzymaniowych (SLA) w odniesieniu do zaewidencjonowanych licencji oraz urządzeń w zakresie co najmniej: nazwa, okres, data dokumentu, numer dokumentu, dostawca, osoba kontaktowa, wartość, opis, warunki oraz umożliwiać dołączenie dowolnej ilości załączników z repozytorium i powiązanie umowy utrzymaniowej z dowolną ilością zasobów (urządzenia, licencje).

10. Ochrona danych (DLP)

- 1) System automatycznie tworzy listę podłączanych do komputerów urządzeń USB.
- 2) System automatycznie klasyfikuje podłączane urządzenia (pamięć masowa, pendrive, aparat fotograficzny, urządzenie multimedialne itp.)
- 3) System umożliwia uzyskanie informacji kto, kiedy i na jakim komputerze posługiwał się urządzeniem zewnętrznym, pozwalając na jego jednoznaczne zidentyfikowanie.
- 4) System umożliwia utworzenie listy urządzeń USB dozwolonych do stosowania - tzw. białej listy urządzeń USB.
- 5) System ma możliwość zidentyfikowania urządzenia USB i wprowadzenia go do systemu za pośrednictwem konsoli administracyjnej oraz wbudowanego do konsoli oprogramowania/skryptu, pozwalając na zidentyfikowanie jednocześnie wielu urządzeń USB (multiplexer USB).
- 6) System musi umożliwiać zdefiniowanie reguł stanowiących podstawę użytkowania urządzeń USB (dozwolone/niedozwolone) na inwentaryzowanych komputerach wg kryteriów: użytkownik, dzień tygodnia, okres (data od, godzina od, data do, godzina do), urządzenie USB, komputer, data obowiązywania reguły

11. Zdalna administracja komputerami

- 1) System ma automatycznie wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika.
 - a. System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu Windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania.
 - b. Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi,

- wyłączenie/włączenie/restart zapory Windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego.
- c. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status).
 - d. System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, Windows PowerShell. System posiada co najmniej 70 predefiniowanych poleceń. System musi umożliwiać użytkownikom automatyczne definiowanie poleceń cmd/PowerShell. Funkcjonalność ta pozwala na wprowadzanie opisów zadanych czynności, a następnie, wykorzystując zaawansowane algorytmy AI, system automatycznie generuje adekwatne skrypty.
 - e. Zaawansowany Asystent AI do Przygotowywania Skryptów do precyzyjnego tworzenia szczegółowych skryptów
 - f. System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.).
 - g. System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako)
 - h. System musi umożliwiać tworzenie zadań cyklicznych dla komputerów.
 - i. Obsługa zadań cyklicznych musi następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia, pierwszy/drugi/trzeci/czwarty/ostatni poniedziałek/wtorek/środa/czwartek/piątek/sobota/niedziela/dzień wolny/dzień powszedni co n miesięcy, nowe zadanie n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu, w pierwszy/drugi/trzeci/czwarty/ostatni, w dowolny dzień tygodnia, dzień wolny/dzień powszedni wybranego miesiąca, nowe zadanie n lat od wykonania.
 - j. System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie.
- 2) System musi posiadać wbudowany skaner wyposażony w harmonogram skanowania umożliwiający wykrywanie (rozpoznawanie) komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro.
- a. System musi umożliwiać zarządzanie komputerami z technologią Intel vPro, w tym: Serial Over LAN, zdalne włączanie, wyłączenie komputera, zdalna konfiguracja BIOS, uruchomienie zdalnie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji.
 - b. System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym (od VPro v.6).
- 3) System musi umożliwiać za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacją oprogramowania, poprawek i aktualizacji (service pack, patch).

- a. System umożliwia zdalne połączenie do wielu komputerów jednocześnie i podgląd oraz operowanie na pulpitach tych komputerów w technologii Ultra VNC.
 - b. System musi umożliwiać uruchomienie do 6 sesji Ultra VNC na jednym ekranie.
 - c. System musi umożliwiać uruchomienie sesji Ultra VNC w trybie połączenia się do obecnie zalogowanego użytkownika oraz w trybie RDP (wylogowania użytkownika i przejęcia dostępu).
12. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.
13. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.
14. Zdalne Zarządzanie Zaporą (Firewall)
 - 1) System powinien umożliwiać monitorowanie stanu zapory w czasie rzeczywistym, zapewniając aktualne informacje o jej działaniu.
 - 2) System powinien zapewniać zdalne sterowanie zaporą na dowolnych komputerach, co obejmuje:
 - a. Definiowanie i zarządzanie złożonymi zasadami zapory z centralnego panelu administracyjnego.
 - 3) System powinien umożliwiać szybkie identyfikowanie i reagowanie na potencjalne zagrożenia, zwiększając bezpieczeństwo sieci.
 - 4) System powinien oferować kontrolę ruchu sieciowego, umożliwiając zarządzanie dostępem do zasobów sieciowych.
15. Automatyzacja
 - 1) System ma mieć możliwość ustalania harmonogramu, zgodnie z którym uruchamiane są czynności konserwacyjne, naprawcze, porządkujące.
 - 2) Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania danej czynności (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartości parametrów wejściowych, a także zatrzymania/uruchomienia harmonogramu uruchomienia dla każdej z czynności.
 - 3) System musi mieć możliwość definiowania czynności wykonywanych automatycznie.
 - 4) System musi być wyposażony w następujące mechanizmy automatyzacji: wykonywanie kopii bezpieczeństwa bazy danych, identyfikacja aplikacji i pakietów, porządkowanie bazy danych / odbudowa indeksów, usuwanie nadmiarowych danych w bazie danych, usuwanie zewnętrznych plików (logów).
 - 5) System musi być wyposażony w mechanizmy informowania - wysyłania komunikatów (alerty) o: zasobach zakazanych (pliki erotyczne i pornograficzne), zasobach multimedialnych (pliki multimedialne), nowych komputerach w bazie danych, braku skanowania komputerów, brakach w licencjach, niewłaściwych datach systemowych komputerów, urządzeniach bez użytkowników, zdublowanych systemach operacyjnych, zakazanych procesach/stronach www /aplikacjach, wygasaniu serwisu lub licencji, przekroczeniu wielkości bazy danych, nadmiernym obciążeniu dysków twardych, nadmiernym obciążeniu sieci, nadmiernym obciążeniu sieci na komputerze, nadmiernym obciążeniu procesora, nadmiernym obciążeniu pamięci RAM, małej ilości wolnego miejsca na dysku, upływającej gwarancji,
16. Zarządzanie magazynem IT
 - 1) System musi umożliwiać obsługę magazynu IT.
 - 2) System musi umożliwiać obsługę dowolnej ilości magazynów w różnych lokalizacjach.

- 3) System musi umożliwiać obsługę dokumentów PZ, RW, WZ, MM+, MM-, LI.
 - 4) System musi prowadzić ewidencję materiałów w magazynach w oparciu o metodę FIFO (pierwsze przyszło, pierwsze wyszło).
 - 5) System musi umożliwiać obsługę kodów kreskowych dla materiałów w magazynach.
 - 6) System musi udostępniać informację o wartościach materiałów w poszczególnych magazynach, stanach materiałów w magazynach, dokumentach dotyczących danego materiału w dowolnym magazynie.
 - 7) System musi umożliwiać automatyczne łączenie wygenerowanych dokumentów z zasobami systemu, takimi jak osoby, urządzenia.
 - 8) System musi zapewniać możliwość przeglądu wszystkich wygenerowanych dokumentów.
17. Repozytorium
- 1) Konsola administracyjna musi być wyposażona w repozytorium dokumentów dowolnego typu.
 - 2) Repozytorium musi umożliwiać: dodawanie nowych dokumentów dowolnego typu, przeszukiwanie, oznaczanie dokumentów (znaczniki TAG) więcej niż jednym znacznikiem, podgląd dokumentów, dołączanie dokumentów z repozytorium w dowolnym miejscu systemu, uzyskanie informacji w jakich miejscach systemu dany dokument repozytorium występuje.
 - 3) Repozytorium musi umożliwić definiowanie kontenerów na dokumenty.
18. Kody kreskowe
- 1) System wspiera obsługę kodów kreskowych jedno i dwuwymiarowych.
 - 2) System wspiera parametryzację kodu w zakresie wielkości graficznej kodu.
 - 3) System pozwala w każdym momencie na zmianę typu i atrybutów kodu.
 - 4) System informuje o błędzie generacji kodu, np. na skutek niewłaściwej długości wprowadzonego ciągu znaków w stosunku do danego standardu kodu.
 - 5) Istnieje możliwość podglądu kodu oraz jednostkowego i masowego wydruku kodu / kodów.
 - 6) System musi generować kody kreskowe (jedno i dwuwymiarowe) dla każdego zaewidencjonowanego urządzenia w standardzie wybranym przez użytkownika: aztec, codabar, code128, code39, dataMatrix, EAN128, EAN13, EAN8, interleaved2of5, ITF14, PDF417, POSTNET, qrcode, royalMailCBC, UPCA, UPCE, USPSIntelligentMail.
 - 7) Obsługa kodów kreskowych nie może wymagać instalacji czcionek.
 - 8) Parametry kodu kreskowego (wymiary, wielkość i typ czcionki) muszą być definiowalne.
19. Wysyłanie wiadomości
- 1) Komunikator
 - a. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości pomiędzy użytkownikiem komputera z zainstalowanym Klientem a administratorem systemu.
 - b. Powinien zapewniać możliwość inicjowania czatu przez administratora.
 - c. Użytkownik powinien mieć opcję rozpoczęcia rozmowy za pomocą ikony na pasku zadań, która automatycznie uruchamia się zgodnie z konfiguracją Klienta.
 - d. System musi przechowywać historię konwersacji.
 - e. Powinien informować administratora poprzez powiadomienie w konsoli systemowej o nowych wiadomościach od użytkowników.
 - 2) Wiadomość Jednorazowa:

- a. System powinien umożliwiać wysyłanie jednorazowych wiadomości w trybie natychmiastowym jako ALERT.
 - b. Musi oferować możliwość wystania wiadomości z opcją odłożenia na później (na 10 minut, 1, 2, 4 godziny) dla późniejszego odczytu.
 - c. Powinien zapewniać historię wysyłania i odbierania wiadomości przez użytkowników, z możliwością edycji treści w edytorze HTML.
 - d. Wiadomość powinna być dostępna do wystania do określonej grupy, wybranych komputerów lub użytkowników.
 - e. System musi umożliwiać konfigurację czasu wygaśnięcia wiadomości.
- 3) Wiadomości Cykliczne:
- a. Powinien pozwalać na tworzenie szablonów wiadomości do regularnego użytku.
 - b. Musi zapewniać funkcję odłożenia wysyłania wiadomości dla późniejszego odczytu, z możliwością edycji treści w edytorze HTML.
 - c. System powinien rejestrować historię wysyłania i odczytywania wiadomości przez użytkowników.
 - d. Powinien umożliwiać wystanie wiadomości do zdefiniowanej grupy, wybranych komputerów lub użytkowników.
 - e. Musi oferować opcję konfiguracji terminu, po którym wiadomość wygaśnie.
- 4) System szkolenia pracowników za pomocą wiadomości.
- a. System musi mieć możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urzędów i użytkowników komputerów.
 - b. System musi posiadać predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa”, „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa”, „Postępowanie w przypadku naruszenia tajemnicy”, „Udostępnienie informacji stanowiących tajemnicę”.
 - c. Formatowanie treści musi być zgodne z HTML.
 - d. System musi mieć możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych).
 - e. System musi mieć programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców.
 - f. Użytkownik otrzymujący wiadomość musi być powiadamiany wizualnie i dźwiękowo o otrzymaniu nowej wiadomości.
 - g. Użytkownik musi mieć możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania.
 - h. System musi udostępnia historię przesyłania wiadomości i odczytywania wiadomości przez użytkowników.
 - i. System musi generować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem).
20. System musi posiadać możliwość eksportu / importu treści.
21. Monitorowanie drukarek sieciowych i wydruków
- 1) System musi posiadać możliwość ewidencji wszystkich generowanych wydruków niezależnie od miejsca ich generowania oraz typu drukarki (lokalna, sieciowa).
 - 2) Ewidencja wydruków musi obejmować: nazwę i wielkość dokumentu, datę i godzinę wydruku, nazwę użytkownika drukującego, IP i nazwę komputera, z którego dokonano wydruku, format dokumentu, informację i jedno bądź dwustronnym wydruku, informację o wydruku mono/kolor.
 - 3) System dla każdego wydruku, dla każdej drukarki musi obliczać rzeczywisty koszt wydruku w oparciu o wbudowany definiowalny przez

administratora systemu, cennik wydruków obejmujący cenę papieru (w zależności od formatu) oraz cenę materiałów eksploatacyjnych (toner, tusz) dla danej drukarki, typu wydruku, rozmiaru papieru.

- 4) System musi generować zestawienia pozwalające ustalić miejsca powstawania kosztów wydruków (komórki organizacyjne, użytkownicy) oraz stopień obciążenia poszczególnych urządzeń drukujących.
- 5) System musi prognozować ilość i koszt wydruków na wszystkich drukarkach w okresie kolejnych 3,6,12 miesięcy.
- 6) System musi pozwalać na grupowanie (kojarzenie) drukarek wg sterowników.
- 7) Dla każdej z drukarek SNMP system musi udostępniać informacje: nr seryjny, IP, MAC, bieżący status drukarki, całkowitą ilość wydrukowanych stron, ilość wydrukowanych stron od uruchomienia, błędy, alerty, dostępne porty, stan pokryw, interfejsów sieciowych, rodzaj i ilości pamięci całkowitej i wykorzystanej, informacje o poziomie materiałów eksploatacyjnych

22. Monitorowanie stron www

- 1) System musi posiadać możliwość monitorowania odwiedzanych stron www niezależnie od typu używanej przeglądarki internetowej.
- 2) Ewidencja otwieranych stron musi dotyczyć wielu jednocześnie otwartych zakładek.
- 3) Ewidencja otwieranych stron musi działać również, gdy otwierana jest strona z połączeniem szyfrowanym (https).
- 4) Ewidencja musi obejmować co najmniej: nazwę i adres IP komputera, nazwę użytkownika, datę i godzinę, adres strony, łączny czas korzystania, czas aktywności, czas pasywności.
- 5) W oparciu o algorytmy sztucznej inteligencji - machine learning oraz deep learning system umożliwia analizę treści stron www oraz przypisanie im – w oparciu o treść – odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem odwiedzanych stron.
 - a. Każda odwiedzona strona otrzymuje atrybuty: czy SSL, czy jest bezpieczna, czy zawiera przekierowania, czy znajduje się na liście CERT, czy znajduje się na liście stron hazardowych, czy kategoria strony jest bezpieczna, czy jest produktywna.

23. Monitorowanie serwerów WWW

- 1) System musi umożliwiać monitorowanie wybranych serwerów www.
 - a. System musi przedstawiać informację o działaniu wybranych serwerów oraz ich aktywności.
 - b. System musi posiadać możliwość weryfikacji treści (tekstu) dostępnego na monitorowanej stronie.
 - c. System w sposób graficzny musi przedstawiać działanie serwerów WWW wraz z wyszczególnieniem informacji dla każdego wybranego serwera (status, bieżący czas odpowiedzi, średni czas odpowiedzi za ostatnie 12 miesięcy, aktywność za ostatnie 3, 6, 12 miesięcy).

24. Monitorowanie dziennika zdarzeń

- 1) System musi posiadać możliwość monitorowania dziennika zdarzeń wszystkich komputerów.
- 2) System musi pozwalać na zdefiniowanie ewidencji zdarzeń z komputerów na podstawie kategorii zdarzenia.
- 3) Ewidencja musi zawierać: datę i godzinę zdarzenia, nazwę i adres IP komputera, typ zdarzenia, opis zdarzenia.

25. System musi umożliwiać monitorowanie komunikatów Syslog.

26. Monitorowanie pracy komputerów

- 1) System musi posiadać możliwość monitorowania daty włączenia i wyłączenia komputera niezależnie czy znajduje się w sieci lokalnej czy też poza nią i prezentować czas pracy komputera w układzie graficznym.
 - 2) System musi posiadać ewidencję daty i godziny przyłączenia i odłączenia komputera od systemu monitorującego.
 - 3) System musi ewidencjonować zdarzenia związane z logowaniem się użytkowników do danego komputera, również w przypadku podłączania się wielu użytkowników jednocześnie
 - 4) Monitorowanie sesji zdalnych połączeń
 - a. System musi prowadzić ewidencję sesji zdalnych połączeń na każdym komputerze.
 - b. Informacja o nawiązanej sesji musi zawierać co najmniej: nazwę i adres IP komputera, z którego nastąpiło połączenia, nazwę użytkownika nawiązującego połączenie, nazwę i adres IP komputera docelowego, adres portu połączenia.
27. Monitorowanie sensorów
- 1) System musi umożliwić integrację z systemem monitoringu warunków środowiskowych poprzez odczyt wartości z wykorzystaniem SNMP.
 - 2) Czujniki muszą być grupowane wg typu oraz lokalizacji.
 - 3) System musi prezentować położenie czujników na mapie wbudowanej w system.
 - 4) System musi umożliwić odczyt informacji z czujników temperatury, wilgotności oraz odczytywać zmiany stanu czujników zalania oraz otwarcia drzwi.
 - 5) System musi przechowywać odczytane dane w bazie danych przez zadany okres.
 - 6) System musi umożliwić wysyłanie alertów poprzez email, sms oraz prezentować informację w konsoli o przekroczeniu monitorowanych parametrów.
 - 7) System musi umożliwić graficzną prezentację danych zebranych z monitorowanych czujników.
28. Repozytorium CMDB
- 1) System musi posiadać wbudowaną centralną bazę systemu umożliwiającą import i eksport danych zarówno poprzez API jak też za pomocą wbudowanego import/eksportu, na którą składają się:
 - a. Active Directory - lista skonfigurowanych z konsolą serwerów LDAP, z których są importowane i aktualizowane dane o użytkownikach. System pozwala na wprowadzanie dowolnej ilości serwerów dla różnych domen.
 - b. Kontenery dokumentów - grupy, do których można przypisywać zapisane w systemie dokumenty w celu sortowania.
 - c. Kategorie aplikacji - lista kategorii, do których przynależą wykorzystywane przez użytkowników aplikacje.
 - d. Budżet - zestawienie typów budżetów (kosztów) zaewidencjonowanych w systemie.
 - e. Komputery - lista zinwentaryzowanych komputerów, podzielonych wg typu autoryzacji. Widok rekordu zawiera szczegółowe dane dotyczące danego komputera.
 - f. Dokumenty - repozytorium dokumentów zapisanych w systemie.
 - g. eLearning - zdefiniowane wiadomości typu eLearning. Wykorzystywane są do wysyłania użytkownikom szkoleń wbudowanych w system, zgodnie ze zdefiniowanym harmonogramem.

- h. Kategorie plików - lista typów plików kategoryzowanych przez system. Administrator ma możliwość zdefiniowania własnych grup, do których pliki będą przydzielane, według wpisanej maski.
 - i. Pliki - lista zinwentaryzowanych plików ze wszystkich komputerów.
 - j. Licencje - zestawienie licencji zapisanych w bazie systemu, które administrator może przypisywać do poszczególnych użytkowników.
 - k. Typy licencji - lista typów licencji.
 - l. Lokalizacje - lista zdefiniowanych lokalizacji, do których administrator może przypisać poszczególnych użytkowników. W odróżnieniu od struktury organizacyjnej dane nie są importowane z Active Directory.
 - m. Typy urządzeń - lista typów urządzeń.
 - n. Urządzenia - lista urządzeń podzielonych wg typu.
 - o. Producenci / Dostawcy - lista producentów i dostawców.
 - p. Pamięć masowa - zestawienie dysków twardych z komputerów.
 - q. Porty sieciowe - lista monitorowanych portów sieciowych.
 - r. Usługi sieciowe - lista monitorowanych usług sieciowych.
 - s. Udostępnione zasoby sieciowe - lista udostępnionych zasobów sieciowych.
 - t. Sieci - lista definiowalnych ręcznie sieci, do których administrator może ręcznie przypisywać komputery.
 - u. Systemy operacyjne - zestawienie unikalnych systemów operacyjnych.
 - v. Struktura org. - zestawienie struktur organizacyjnych zdefiniowanych bądź importowanych z Active Directory.
 - w. Kategorie procesów - lista kategorii, do których będą przypisywane procesy aplikacji uruchamianych przez użytkowników. Klasyfikacja procesów odbywa się za pomocą algorytmów sztucznej inteligencji.
 - x. Serwery - lista zinwentaryzowanych serwerów.
 - y. Usługi - zestawienie usług działających na komputerach.
 - z. Oprogramowanie - lista zinwentaryzowanego i monitorowanego oprogramowania.
 - aa. Pamięć masowa USB - lista urządzeń pamięci masowej USB.
 - bb. Administratorzy - lista administratorów systemu,
 - cc. Użytkownicy / pracownicy - lista pracowników.
 - dd. Kategorie WWW - lista kategorii stron WWW wykorzystywanych w procesie klasyfikacji stron internetowych. Klasyfikacja oparta o sztuczną inteligencję.
 - ee. Serwisy WWW - lista monitorowanych serwisów WWW.
29. Worktime manager
- 1) System musi być wyposażony w zestaw statystycznych danych o pracy użytkownika i zdefiniowanych grup użytkowników.
 - 2) System musi umożliwiać definiowanie dowolnej ilości grup użytkowników przypisanych do dowolnej ilości przełożonych.
 - a. System musi umożliwiać prezentację szczegółowych informacji o przypisanej grupie bezpośrednio w panelu pracownika na pulpicie przełożonego, który jest przypisany do tej grupy.
 - 3) Dane muszą być prezentowane w formie interaktywnych widgetów oraz w formie danych analitycznych.
 - 4) Dane dla grup użytkowników muszą być skumulowane oraz analityczne.
 - a. Prezentacja danych odbywa się poprzez wskazanie pracownika lub grupy pracowników oraz wybranie okresu danych źródłowych.
 - b. Informacje prezentowane w panelu: informacja o otwartych sesjach, informacja o sesjach historycznych, informacja o czasie zalogowania użytkownika, informacja o czasie pracy komputera, informacja o aktywności użytkownika w aplikacjach, informacja o produktywności

użytkownika w aplikacjach, informacja o produktywności, wykorzystywanych aplikacjach, odwiedzonych stronach www z podziałem na kategorie stron, informacja o uruchomionych procesach z podziałem na kategorie, informacja o aktywności na stronach www, informacja o wykonanych wydrukach (nazwa dokumentu, data i godzina wydruku, drukarka, ilość stron, rodzaj wydruku – czarno-biały czy w kolorze, koszt wydruku), informacja o transferze sieciowym, informacja o zależności czasu pracy w trybach: zalogowany/ uśpiony/ wylogowany.

- 5) System musi umożliwić wyświetlanie informacji o użytkowniku pobranych z Active Directory. Informacje powinny być aktualizowane zgodnie z harmonogramem połączenia z domeną.
 - 6) System musi prezentować w formie tabelarycznej informacje o dokumentach (np. protokoły przekazania i zwrotu sprzętu), komputerach i urządzeniach, które zostały przypisane użytkownikowi.
 - 7) System musi posiadać widżety prezentujące dane w wybranym przedziale czasu: czas zalogowania – dni, czas pracy komputera – dni, aktywność w aplikacjach, produktywność w aplikacjach, produktywność w czasie pracy, czas pracy w aplikacjach, czas spędzony na stronach www wg kategorii stron, czas spędzony w aplikacjach (procesach) wg kategorii procesu, czas aktywności na stronach www, stron wydruku wg dokumentów, transfer sieciowy, czas pracy wg zalogowany/ wylogowany / uśpiony, czas aktywności w godzinach pracy.
30. Raportowanie i eksport danych
- 1) Systemu musi umożliwiać wyeksportowania wybranych lub wszystkich danych do formatu xls, csv, OpenOffice calc, html, mht, xml, jpeg, png, gif, bmp.
 - 2) System musi mieć możliwość kategoryzowania raportów (spośród wszystkich raportów) oraz dodawania raportów użytkownika (zaprojektowanych przez użytkownika).
 - 3) System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów.
 - 4) Generowanie raportu musi odbywać się po stronie serwera a nie klienta.
 - 5) System musi umożliwiać wieloinstancyjność raportowania (wiele otwartych raportów jednocześnie z wielu widoków).
 - 6) System musi mieć możliwość generowania i wyświetlania dowolnych wieloparametrycznych raportów w standardzie SAP Crystal Reports (rpt) oraz Stimulsoft.
 - 7) System musi umożliwiać eksport danych z raportu do formatów: RPT, PDF, XLS, DOC, RTF.
 - 8) System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu).
 - 9) System musi posiadać co najmniej 150 zdefiniowanych raportów dotyczących obszarów funkcjonalnych
31. System musi zapewnić interfejs API.
- 1) System musi udostępniać możliwości komunikacji z systemem za pomocą REST API.
 - 2) Komunikacja z REST API musi odbywać się w sposób szyfrowany min. Protokołem TLS 1.3 i chroniony kluczem alfanumerycznym.
 - 3) System musi zapewniać możliwości modyfikacji i dostosowania klucza zabezpieczeń REST API i pozwalać na ustanowienie klucza o długości co najmniej 32 znaków.

- 4) System musi pozwalać na tworzeniu requestów obsługujących parametry w formacie JSON.
- 5) W ramach REST API konieczne musi być możliwość pobierania danych ze wszystkich tabel systemu, zawierających dane merytoryczne.
- 6) System musi przyjmować requesty pozwalające na umieszczanie danych w systemie za pomocą REST API.
- 7) System musi dopuszczać komunikację złożoną, za pomocą sekwencji requestów REST API.
- 8) System musi pozwalać na automatyczną komunikację za pomocą REST API z innymi systemami z wykorzystaniem składni API systemu.

32. System musi umożliwiać generowanie powiadomienia

System musi posiadać dokumentację w postaci min. 20 filmów instruktażowych/nagrań z webinarów w języku polskim.

System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim

Wsparcie i pomoc

Gwarancja i aktualizacja oprogramowania

18 miesięcy, nie dłużej niż do dnia 30.06.2026r.

III.II. UG.2 Oprogramowanie oraz monitoring usług i użytkowanych systemów

Przez wdrożenie systemu monitorowania Zamawiający rozumie dostawę licencji, zaprojektowanie systemu oraz jego uruchomienie, a także przeprowadzenie instruktażu z zakresu administracji i jego obsługi.

System monitorowania ma stanowić narzędzie pozwalające na gromadzenie i analizowanie danych dotyczących różnorodnych zdarzeń związanych z użytkowaniem przez Zamawiającego systemami teleinformatycznymi wraz z powiadamianiem zespołów bezpieczeństwa.

Zaproponowane rozwiązanie powinno wspierać zespół monitorowania w procesie reakcji na wykryte incydenty. System ma przetwarzać dane zarówno w celu bezpośredniego monitorowania systemów i usług jak i także w celu wsparcia procesu utrzymywania zgodności z regulacjami prawnymi oraz standardami bezpieczeństwa, w szczególności w celu wypełnienia obowiązków wynikających z:

- Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,
- Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych,
- Ustawy z dnia 10 listopada 2020 r. o doręczeniach elektronicznych
- Rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej,
- Ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
- Ustawy z dnia 5 września 2016 r. o usługach zaufania i identyfikacji elektronicznej,
- Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną,
- Ustawę z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach,
- Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych.

parametr

Wykrywanie i monitorowanie

charakterystyka [wymagania minimalne]

Monitorowanie infrastruktury IT, w tym serwerów i usług.
System pozwala na monitorowanie zdefiniowanych zdarzeń, w tym zbieranie, analizowanie i wizualizację danych.
System jest przystosowany do przetwarzania danych typowych dla systemów teleinformatycznych:

- Adresy IP4 i IP6

Interfejs i prezentacja danych

- Nazwy DNS
- Identyfikatory protokołów sieciowych np. SNMP, SSH, TELNET, IPMI, JPM, HTTP/HTTPS, VMWare
- Porty
- Nazwy i identyfikatory użytkowników
- Nazwy i identyfikatory procesów
- Nazwy i identyfikatory zasobów
- Czasu
- i innych

System umożliwia wykrywanie wszelkich problemów w infrastrukturze Zamawiającego i powiadamia wskazanych użytkowników

System zapewnia graficzny interfejs użytkownika dostępny wyłącznie za pomocą przeglądarki internetowej.

System wspiera generowanie mapy monitorowane środowiska uwzględniającej prezentację co najmniej urządzeń, portów, prędkości połączeń i nazw urządzeń.

System prezentuje dane na wykresach w czasie rzeczywistym.

System pozwala na tworzenie własnych wykresów gromadzących i prezentujących wiele danych.

Interfejs użytkownika wyodrębnia prezentację co najmniej następujących danych:

- problemy
- hosty
- mapy
- usługi
- SLA
- Zasoby
- Raporty
- Kolekcje danych
- Alerty
- Administracja i zarządzanie, w tym zarządzanie użytkownikami.

System musi udostępniać ogólnodostępną wyszukiwarkę, która w łatwy sposób pozwala odnaleźć hosty, grupy i schematy.

System pozwala na tworzenie własnych motywów interfejsu użytkownika.

System pozwala na rebranding obejmujących co najmniej możliwość wstawienia własnego loga.

Zarządzanie monitorowanymi zasobami

System pozwala na zarządzanie użytkownikami korzystającymi z interfejsu przeglądarkowego.

Użytkownicy mogą pełnić różne role w systemie oraz należeć do wielu grup użytkowników.

Uprawnienia w systemie muszą pozwalać na przydzielenie dostępu do:

- dashboardu
- monitoringu procesów, hostów, mapy
- usług i weryfikacji poziomu SLA
- zasobów w tym serwerów
- raportów i notyfikacji
- kolekcji gromadzonych danych
- alertów
- API

System umożliwia zarządzania hostami, w tym przydzielanie ich do grup i stosowanie dla nich wbudowanych standardowych schematów (templates) monitorowania.

System pozwala na definiowanie i zarządzanie monitorowanymi parametrami.

System oferuje minimum 50 monitorowanych parametrów obejmujących co najmniej następujące grupy/typy:

Raportowanie i
alarmowanie
licencjonowanie

- Jądro systemu (kernel)
- Monitorowanie logów
- Parametry dotyczące sieci
- Procesy
- Czujniki sprzętowe
- Parametry systemu
- System plików
- Pamięć
- Strony internetowe

System pozwala na tworzenie własnych skryptów oraz definiowanych własnych triggerów wyzwalających zdarzenie za pomocą obsługiwanych przez system wyrażeń regularnych.

Wyrażenia muszą obsługiwać funkcje, ich parametry i operatory. Liczba oferowanych funkcji – min. 50 i operatorów – min. 10.

System musi posiadać możliwość tworzenia własnych schematów monitorowania.

System musi pozwalać na definiowanie pożądanych parametrów SLA.

System musi posiadać wbudowane narzędzia monitorowania środowiska VMWare

System pozwala na przesyłanie notyfikacji/powiadomień dla zdefiniowanych zdarzeń poprzez email z wykorzystaniem serwera/ usługi Zamawiającego

Zamawiający wymaga dostarczenia licencji wieczystej z prawem do aktualizacji. Licencja na System nie może narzucać jakichkolwiek dodatkowych wymagań dla Zamawiającego skutkujących ponoszeniem dodatkowych kosztów związanych z jej utrzymaniem.

Licencja musi obejmować wszystkie funkcjonalności zaoferowanego oprogramowania i pozwalać na monitorowanie dowolnej liczby urządzeń infrastruktury, serwerów i usług IT.

Licencja nie może w żaden sposób być przypisania do użytkownika, serwera czy maszyny. Nie może być także uzależniona od liczby rdzeni procesora.

Licencja musi pozwalać na zainstalowanie oprogramowania w dowolnej liczbie instancji – ma być licencją udzieloną na Zamawiającego, bez ograniczania liczby instalacji oprogramowania.

Wsparcie techniczne

Gwarancja producenta i wsparcie techniczne - nie później niż do 30.06.2026r. obejmująca:

dostarczanie aktualizacji Systemu, udzielanie konsultacji telefonicznych / mailowych w zakresie funkcjonowania i konfiguracji Systemu oraz jego rozszerzania

Minimalny zakres
monitorowanych
systemów i usług - źródła
danych

W ramach wdrożenia Systemu monitorowaniem objęte zostaną następujące źródła zdarzeń:

Serwery i aplikacje kluczowych baz danych – 1 szt.

Serwer WWW – 1 szt. (www/bip)

Urządzenie brzegowe – 1 szt.

Serwer poczty elektronicznej 1 szt.

Switch (SNMP) – min. 1 szt.

Monitorowanie integracji z systemem ePUAP – 1 szt.

Monitorowanie integracji z systemem eDoręczeń – 1 szt.

Sumarycznie przewiduje się podłączenie nie więcej niż 7 źródeł danych rozumianych jako serwer/urządzenie sieciowe, generujących różne rodzaje zdarzeń w liczbie szacunkowo kilku tysięcy na dobę.

Zakres prac i wdrożenia

8. Zebranie informacji dotyczących monitorowanej infrastruktury, monitorowanych źródeł danych.

9. Instalację i konfigurację systemu w zasobach informatycznych Zamawiającego – preferowane środowisko Linux
10. Uzgodnienie i wdrożenie sposobu backupu Systemu.
11. Dostarczenie licencji na System.
12. Uzgodnienie mechanizmów funkcjonalnych z Zamawiających oraz ich wdrożenie.
13. Przeprowadzenie instruktażu/warsztatu szkoleniowego w wymiarze 2h
14. Skonfigurowanie i uruchomienie mechanizmów powiadomień o zdarzeniach krytycznych.

CZĘŚĆ IV

REALIZACJA W RAMACH ETAPU I

GMINNY OŚRODEK POMOCY SPOŁECZNEJ

IV.I.GOPS.1 Usługa chmurowa dla backup baz danych

Lp. charakterystyka [wymagania minimalne]

1. Usługa do wykonywania backupu online oraz do bezpiecznego przechowywania i udostępniania różnego rodzaju danych na okres 18 miesięcy, nie dłużej niż do dnia 30.06.2026
2. Dostępna przestrzeń – min. 200GB
3. Gwarantowany dostęp dla 5 użytkowników
4. Poza wykonywaniem kopii zapasowych baz danych MS SQL i PostgreSQL, aplikacja umożliwi backup plików i folderów znajdujących się zarówno na komputerze lokalnym, jak i w lokalizacji sieciowej dostępnej za pomocą protokołów FTP i SMB.
Wymagany jest prosty i elastyczny kreator zadań backupu pozwalający na dostosowanie cyklu w jakim kopia zapasowa będzie przesyłana do certyfikowanej chmury
5. System ma pozwalać na udostępnianie plików oraz zabezpieczanie ich hasłem lub generowanym kluczem szyfrującym
6. Dostęp do danych będzie możliwy przez przeglądarkę internetową, aplikację desktopową oraz aplikacje mobilne (Android, iOS).

REALIZACJA W RAMACH ETAPU II

URZĄD GMINY W WIELKIEJ NIESZAWCE

IV.II.UG.1 Usługa chmurowa dla backup baz danych

Lp. charakterystyka [wymagania minimalne]

1. usługa do wykonywania backupu online oraz do bezpiecznego przechowywania i udostępniania różnego rodzaju danych na okres 18 miesięcy, nie dłużej niż do dnia 30.06.2026
2. Dostępna przestrzeń – min. 1TB
3. Gwarantowany dostęp dla 15 użytkowników
4. Poza wykonywaniem kopii zapasowych baz danych MS SQL i PostgreSQL, aplikacja umożliwi backup plików i folderów znajdujących się zarówno na komputerze lokalnym, jak i w lokalizacji sieciowej dostępnej za pomocą protokołów FTP i SMB.

- Wymagany jest prosty i elastyczny kreator zadań backupu pozwalający na dostosowanie cyklu w jakim kopia zapasowa będzie przesyłana do certyfikowanej chmury
- System ma pozwalać na udostępnianie plików oraz zabezpieczanie ich hasłem lub generowanym kluczem szyfrującym
 - Dostęp do danych będzie możliwy przez przeglądarkę internetową, aplikację desktopową oraz aplikacje mobilne (Android, iOS).

CZĘŚĆ V

URZĄD GMINY W WIELKIEJ NIESZAWCE

V.UG.1 System do backupu

Kompleksowe, zintegrowane rozwiązanie do backupu wraz z usługą wdrożenia zdalnego oraz pomocą techniczną wykonawcy na okres min. 18 miesięcy, nie dłużej niż do dnia 30.06.2026r.

W zastosowanym rozwiązaniu oprogramowanie do centralnego zarządzania backupem ma być zintegrowane z platformą sprzętową serwera NAS tak aby nie było potrzeby instalacji serwera backupu (serwera zarządzania) na osobnym serwerze

System powinien umożliwić archiwizację 28 stacji roboczych.

Zamawiający wymaga dostarczenia i wdrożenia rozwiązania składającego się z urządzenia NAS, dysków twardych oraz oprogramowania do backupu spełniających poniższe wymagania.

<i>parametr</i>	<i>charakterystyka [wymagania minimalne]</i>
<i>Procesor</i>	Jeden 4-rdzeniowy/8-wątkowy AMD Ryzen V1500B lub równoważny procesor osiągający w testach PassMark - CPU Mark wynik nie gorszy niż 4600 pkt. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie https://www.cpubenchmark.net (z dnia ogłoszenia postępowania lub nowszy).
<i>Pamięć RAM</i>	16 GB DDR4 SODIMM ECC z opcją rozszerzenia do 32GB pamięci SO-DIMM DDR4 ECC
<i>Ilość obsługiwanych dysków</i>	8 dysków o maksymalnej pojemności 20 TB każdy, po podłączeniu 2 modułów rozszerzających do 18 dysków; 2 dyski M.2 NVMe 2280
<i>Zamontowane dyski twarde</i>	Osiem dysków twardych o pojemności 12 TB każdy znajdujące się na liście kompatybilności producenta oferowanego urządzenia NAS spełniające wymagania: - pamięć podręczna min. 256 MB - prędkość obrotowa min. 7200 obr/min - min. 1 mln godzin MTBF - czujnik drgań ruchu obrotowego
<i>Interfejsy sieciowe</i>	4 x RJ-45 (10/100/1000)
<i>Porty</i>	4 x USB 3.2 Gen 1, 2 x eSATA
<i>Obsługa RAID</i>	Basic, JBOD, RAID 0,1,5,6,10, SHR + Obsługa Hot Spare dla SHR, RAID 1,5,6,10
<i>Funkcje RAID</i>	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
<i>Szyfrowanie</i>	Możliwość szyfrowania wybranych udziałów sieciowych.

na Rozwój Cyfrowy

Protokoły

Usługi

Obsługa SSD Cache

Obsługa migawek

Zarządzanie dyskami

Język GUI

Certyfikaty

System plików

Liczba wolumenów

Liczba celów iSCSI

Liczba iSCSI LUN

Liczba kont użytkowników

Liczba grup

Liczba folderów udostępnionych

Ilość jednoczesnych połączeń

Zasilacz

Chłodzenie

Gwarancja i serwis

Wymagania, które muszą być realizowane przez oprogramowanie do backupu

SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, SNMP, VPN

Serwer VPN

Serwer pocztowy dla kilku domen

Stacja monitoringu

Windows ACL

Integracja z Windows ADS

Firewall z kontrolą ruchu

Serwer WWW

Serwer plików

Manager plików przez WWW

Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie

Usługa DDNS

Oprogramowanie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji Vmware

Wymagane wsparcie dla SSD Cache

- Maksymalna liczba migawek folderów współdzielonych: 1 024
- Maksymalna liczba migawek systemu: 65 536

SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów

Polski

EAC, VCCI, CCC, RCM, KC, FCC, CE, BSMI

Dyski wewnętrzne Btrfs, EXT4. Dyski zewnętrzne Btrfs, FAT, NTFS, EXT3, EXT4, HFS+, exFAT

Do 64

Do 128

Do 256

2048

256

512

1000 dla AFP/NFS/FTP/WebDAV

250 W

FAN x 2 120 mm x 120 mm

3 lata gwarancji door-to-door producenta lub autoryzowanego partnera producenta na urządzenie

3 lata gwarancji door-to-door producenta lub autoryzowanego partnera producenta na dyski

1. Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich
2. Program serwerowy kompatybilny z systemami: Microsoft Windows XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology
3. Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology
4. Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików)

Usługa wdrożenia

5. Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)
6. Automatyczny backup przy wyłączaniu komputera
7. Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych * i ?
8. Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows)
9. Backup baz danych i plików poczty w trybie online i offline
10. Kopie rotacyjne (wersjonowanie)
11. Zapis archiwów w otwartym formacie (ZIP 64-bit)
12. Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi
13. Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore)
14. Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej
15. Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych
16. Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO
17. Kompresja po stronie stacji roboczej
18. Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP,
19. Centralne sterowanie całym Systemem z jednego miejsca
20. Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników
21. Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN
22. Wysyłanie Alertów administracyjnych na e-mail
23. Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych
24. Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki
25. Automatyczna aktualizacja oprogramowania na komputerach zdalnych
26. Bezterminowa licencja - licencja nie może być ograniczona czasowo
27. Interfejs, instrukcja i pomoc techniczna w języku polskim

Usługa może zostać zrealizowana zdalnie, a w jej zakresie muszą zawierać się przynajmniej:

- Wysyłka przygotowanej do wdrożenia macierzy NAS (przeprowadzona integracja z oprogramowaniem do backupu),
- Konfiguracja serwera backupu,
- Przygotowanie paczki instalacyjnej aplikacji klienta backupu,
- Omówienie i konfiguracja zadań backupu dla najważniejszych stacji klienckich,
- Instruktażowe szkolenie administratora z wdrożonego systemu obejmujące przynajmniej omówienie konfiguracji i funkcji konsoli administracyjnej, procesu odzyskiwania danych oraz najlepszych praktyk dla rozwiązań backupowych

V.UG.2 Punkty dostępowe

parametr	charakterystyka [wymagania minimalne]
Interfejs sieciowy	(1) Port RJ45 GbE
Interfejs zarządzania	Ethernet Bluetooth
Metoda zasilania	PoE
Zasilanie	UniFi przetącznik PoE
Obsługiwany zakres napięcia	44—57V DC
Maks. pobór mocy	13W
Maks. moc nadawania	
2.4 GHz	22 dBm
5 GHz	26 dBm
Szybkość przepustowości	
2.4 GHz	573.5 Mbps
5 GHz	4.8 Gbps
Wzmocnienie anteny	
2.4 GHz	4 dBi
5 GHz	6 dBi
Standardy WiFi	802.11a/b/g/n/ac/ax
Bezpieczeństwo sieci bezprzewodowej	WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3)
BSSID	8 na radio
VLAN	802.1Q
Zaawansowane QoS	Limitowanie przepustowości na użytkownika
Izolacja ruchu gości	Obsługiwane
Klienci równoczesni	350+
Obsługiwane Szybkości Przesyłania Danych	
802.11a	6, 9, 12, 18, 24, 36, 48, 54 Mbps
802.11b	1, 2, 5.5, 11 Mbps
802.11g	6, 9, 12, 18, 24, 36, 48, 54 Mbps
802.11n (WiFi 4)	6.5 Mbps do 600 Mbps (MCS0 - MCS31, HT 20/40)
802.11ac (WiFi 5)	6.5 Mbps do 3.4 Gbps (MCS0 - MCS9 NSS1/2/3/4, VHT 20/40/80/160)
802.11ax (WiFi 6)	7.3 Mbps do 4.8 Gbps (MCS0 - MCS11 NSS1/2/3/4, HE 20/40/80/160)
Gwarancja producenta	Min. 12 miesięcy

2. Wymagania dotyczące dostarczanej infrastruktury sprzętowej

- Dostarczony sprzęt powinien być wolny od wad fizycznych i nienoszący oznak użytkowania.
- Wykonawca zobowiązany jest do instalacji sprzętu informatycznego w lokalizacjach określonych przez Zamawiającego. W ramach przedmiotowego zamówienia, Zamawiający wymaga dostarczenia, instalacji oraz konfiguracji sprzętu i oprogramowania systemowego, którego parametry minimalne wskazane zostały powyżej. Zamawiający akceptuje sprzęt oraz oprogramowanie o wyższych (lepszach) parametrach użytkowych lub wykonany w nowszej technologii pod warunkiem, że produkty zaoferowane przez Wykonawcę spełniają wszystkie parametry minimalne.
- Wszystkie oferowane produkty mają pochodzić z oficjalnego kanału dystrybucyjnego producenta, posiadać wszystkie wymagane certyfikaty i oznaczenia oraz spełniać wszystkie wymagane prawem normy. Urządzenia nie mogą się znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.

- d) Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie wcześniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by były nieużywane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji poprawności działania).
 - e) Zamawiający wymaga kompleksowego uruchomienia i zainstalowania dostarczonego sprzętu oraz oprogramowania, w tym m. in.: konfiguracja i instalacja serwerów; podłączenie serwerów oraz pozostałych urządzeń do infrastruktury sieciowej zgodnie z wytycznymi Zamawiającego, instalacja serwerowych systemów operacyjnych; konfiguracja backup serwerów; Przygotowanie podstawowej konfiguracji VLAN-ów; Konfiguracja agregacji łączy zgodnie z wytycznymi Zamawiającego; Włączenie i konfiguracja mechanizmów bezpieczeństwa, takich jak 802.1X oraz ACL; Testy funkcjonalne po zakończeniu konfiguracji.
 - f) Zamawiający wymaga, aby wszystkie dostarczone urządzenia zostały umieszczone (zamontowane) i uruchomione w uzgodnionym przez obie strony terminie. Sposób montażu sprzętu ma być dostosowany do technologii wykonania oraz ma być przeprowadzony zgodnie z zaleceniami producenta. Wykonawca dostarczy wszystkie niezbędne kable połączeniowe, zapewniające transmisję danych z pełną prędkością łączonych portów.
 - g) Konfiguracja logiczna sprzętu (nazwy sieciowe, adresy IP, nazwy i konta użytkowników) ma być przeprowadzona zgodnie z zaleceniami Zamawiającego.
 - h) Prace instalacyjne należy realizować w dni robocze w godzinach pracy urzędu.
 - i) Wykonawca jest zobowiązany do zabrania wszystkich opakowań pochodzących od dostarczonego sprzętu, chyba że warunki gwarancji producenta stanowią inaczej
 - j) Wykonawca jest zobowiązany do przeszkolenia pracowników Zamawiającego w zakresie podstawowej konfiguracji, monitorowania oraz zarządzania dostarczonymi urządzeniami.
2. Rozwiązania równoważne. Ogólne zasady równoważności rozwiązań:
- a) Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
 - b) Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
 - c) Użycie w opisie przedmiotu zamówienia nazw rozwiązań, materiałów i urządzeń służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań.
 - d) Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne.
 - e) Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
 - f) W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
 - g) Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań

technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.

- h) Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.
- i) Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego producentów / produktów rozwiązania. ma wyłącznie Postępowanie charakter się nazwami przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

3. Przedmiotowe środki dowodowe.

W celu potwierdzenia zgodności oferowanych produktów z wymaganiami Zamawiającego w zakresie wskazanym w opisie przedmiotu zamówienia, na podstawie art. 106 ust. 1, w związku z art. 107 ust. 1 ustawy Pzp, Zamawiający żąda złożenia **wraz z ofertą** przedmiotowych środków dowodowych: potwierdzających zgodność zaoferowanych przez Wykonawcę rozwiązań –

- a) dostarczanego oprogramowania – zgodnie z wymaganiami Zamawiającego – tj. próbki oprogramowania podlegającej badaniu czy oferowane oprogramowanie odpowiada wymaganiom Zamawiającego. Szczegółowe wymagania dotyczące zawartości próbki oraz sposób jej badania zawarte są w Załączniku nr 10 do SWZ [dotyczy części III]
- b) certyfikatów, oświadczeń, kart katalogowych wskazanych w opisie przedmiotu zamówienia – zgodnie z wymaganiami Zamawiającego

W odniesieniu do przedmiotowych środków dowodowych Zamawiający akceptuje równoważne przedmiotowe środki dowodowe, jeśli potwierdzają, że oferowane dostawy spełniają określone przez Zamawiającego wymagania, cechy i kryteria. W odniesieniu do certyfikatów i sprawozdań wydanych przez jednostki oceniające zgodność Zamawiający akceptuje odpowiednie przedmiotowe środki dowodowe, inne niż te, o których mowa w SWZ, w szczególności dokumentację techniczną producenta, w przypadku gdy dany Wykonawca nie ma ani dostępu do certyfikatów lub sprawozdań z badań wydanych przez jednostkę oceniającą zgodność ani możliwości ich uzyskania w odpowiednim terminie, o ile ten brak dostępu nie może być przypisany danemu Wykonawcy, oraz pod warunkiem, że dany Wykonawca udowodni, że wykonywane przez niego dostawy lub usługi spełniają wymagania, cechy lub kryteria określone w opisie przedmiotu zamówienia lub kryteriów oceny ofert, lub wymagania związane z realizacją zamówienia.

Zamawiający informuje, że działając na podstawie art. 107 ust. 2 ustawy Pzp przewiduje, że w sytuacji, w której Wykonawca nie złożył przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe są niekompletne, Zamawiający jednokrotnie wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie. Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści przedmiotowych środków dowodowych.

4. Nazwy i kody zamówienia według Wspólnego Słownika Zamówień (CPV):

48820000-2	Serwery
30232000-4 -	Sprzęt peryferyjny
31214100-0	Przetłaczniki
48000000-8	Pakiety oprogramowania i systemy informatyczne
72263000-6	Usługi wdrażania oprogramowania

ROZDZIAŁ 4. TERMIN WYKONANIA ZAMÓWIENIA

Zamówienie będzie wykonane w miejscu siedziby Zamawiającego i Jednostki Podległej, zgodnie z Opisem Przedmiotu Zamówienia.

Wykonawca wykona zamówienie w terminie maksymalnym:

CZĘŚĆ I –	do 60 dni od dnia zawarcia umowy [kryterium oceny ofert]
CZĘŚĆ II –	do 120 dni od dnia zawarcia umowy, w ramach dwóch etapów: Etap I – do 60 dni [kryterium oceny ofert] od dnia zawarcia umowy Etap II – do 120 dni od dnia zawarcia umowy
CZĘŚĆ III –	do 120 dni od dnia zawarcia umowy, w ramach dwóch etapów: Etap I – do 60 dni [kryterium oceny ofert] od dnia zawarcia umowy Etap II – do 120 dni od dnia zawarcia umowy
CZĘŚĆ IV –	do 120 dni od dnia zawarcia umowy, w ramach dwóch etapów: Etap I – do 60 dni [kryterium oceny ofert] od dnia zawarcia umowy Etap II – do 120 dni od dnia zawarcia umowy
CZĘŚĆ V –	do 120 dni od dnia zawarcia umowy [kryterium oceny ofert]

ROZDZIAŁ 5. PODWYKONAWSTWO

1. Wykonawca może powierzyć wykonanie części zamówienia Podwykonawcy pod warunkiem, że posiadają oni kwalifikacje do ich wykonania. Zamawiający nie wskazuje części zamówienia, których dotyczy obowiązek osobistego wykonania przez Wykonawcę.
2. Zamawiający wymaga wskazania w ofercie części zamówienia, której wykonanie Wykonawca zamierza powierzyć podwykonawcom oraz podania nazw firm podwykonawców i wartości lub procentowego udziału usług realizowanych przez danego podwykonawcę.
3. Przez umowę o podwykonawstwo należy rozumieć umowę zawartą w formie pisemnej, o charakterze odpłatnym, której przedmiotem są usługi, dostawy lub roboty budowlane stanowiące część zamówienia publicznego, zawartą między wybranym przez Zamawiającego Wykonawcą, a innym podmiotem (Podwykonawcą), a także pomiędzy Podwykonawcą, a dalszym Podwykonawcą lub pomiędzy dalszymi Podwykonawcami.
4. Jeżeli zmiana lub rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby wykonawca powoływał się w celu wykazania spełniania warunków udziału w postępowaniu, o których mowa w art. 118 ust. 1 ustawy Pzp, wykonawca jest obowiązany wykazać zamawiającemu, iż proponowany inny podwykonawca lub wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż wymagany w trakcie postępowania o udzielenie zamówienia. Przepis art. 122 ustawy Pzp stosuje się.
5. Wykonawca ponosi wobec zamawiającego pełną odpowiedzialność za usługi, które wykonuje przy pomocy podwykonawców, tzn. odpowiada za działania, uchybienia, zaniedbania i zaniechania podwykonawcy w takim samym zakresie jak za działania, uchybienia, zaniedbania i zaniechania własne.
6. Rozliczenia Wykonawcy z Podwykonawcą nie obciążają finansowo i materialnie Zamawiającego.
7. Powyższe zapisy mają zastosowanie także wobec dalszych Podwykonawców.
8. Obowiązki Wykonawcy w zakresie umów z podwykonawcami uregulowane są we wzorze umowy stanowiącym załącznik nr 7 do SWZ.

ROZDZIAŁ 6. KORZYSTANIE PRZEZ WYKONAWCĘ ZE ZDOLNOŚCI TECHNICZNYCH LUB SYTUACJI EKONOMICZNEJ INNYCH PODMIOTÓW

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
2. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, Wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te zrealizują usługi, do realizacji których te zdolności są wymagane.
3. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa wraz z ofertą zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów (załącznik nr 6 do SWZ)
4. Zamawiający ocenia, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu, o których mowa w rozdz. 8 ust. 2 pkt 3 i 4, a także

bada, czy nie zachodzą, wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem Wykonawcy.

5. Podmiot, który zobowiązał się do udostępnienia zasobów, odpowiada solidarnie z Wykonawcą, który polega na jego sytuacji finansowej lub ekonomicznej, za szkodę poniesioną przez zamawiającego powstałą wskutek nieudostępnienia tych zasobów, chyba że za nieudostępnienie zasobów podmiot ten nie ponosi winy.
6. Jeżeli zdolności techniczne lub zawodowe, sytuacja ekonomiczna lub finansowa podmiotu udostępniającego zasoby nie potwierdzają spełniania przez Wykonawcę warunków udziału w postępowaniu lub zachodzą, wobec tego podmiotu podstawy wykluczenia, Zamawiający żąda, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.
7. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia lub w przypadku korzystania z podmiotów udostępniających zasoby na podstawie art. 118 ustawy Pzp Wykonawca lub minimum jeden Wykonawca wspólnie ubiegający się o zamówienie lub minimum jeden podmiot udostępniający zasoby musi posiadać pełne doświadczenie wskazane w warunku udziału w postępowaniu wskazane w SWZ - dotyczy to konieczności wykazania doświadczenia wynikającego z powtarzalności wykonanych usług.
8. Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.

ROZDZIAŁ 7.

OFERTA SKŁADANA PRZEZ WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie niniejszego zamówienia. Wykonawcy występujący wspólnie (np. spółki cywilne, konsorcja), zgodnie z art. 58 ust. 2 ustawy Pzp zobowiązani są ustanowić pełnomocnika do reprezentowania Wykonawcy w postępowaniu o udzielenie zamówienia publicznego albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
2. Wszelka korespondencja oraz rozliczenia prowadzone będą wyłącznie z podmiotem występującym jako Pełnomocnik. Dokument ten winien być opatrzony przez osobę/osoby uprawnioną(-e) do jego udzielenia tj. zgodnie z formą reprezentacji każdego z Wykonawców kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. W przypadku wspólników spółki cywilnej dopuszczalne jest przedłożenie umowy spółki cywilnej, z której wynika zakres i sposób reprezentacji, a w przypadku konsorcjum przedłożenie umowy konsorcjum.
3. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenia, o których mowa w Rozdziale 9 ust. 1 SWZ, składa każdy z wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
4. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika, które roboty budowlane/dostawy/usługi wykonają poszczególni wykonawcy – załącznik nr 8 do SWZ.

ROZDZIAŁ 8.

OPIS WARUNKÓW UDZIAŁU W POSTĘPOWANIU I PODSTAWY WYKLUCZENIA

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na zasadach określonych w SWZ, oraz spełniają określone przez Zamawiającego warunki udziału w postępowaniu.
2. 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.
 - 3) **sytuacji ekonomicznej lub finansowej:**
Zamawiający nie stawia warunku w powyższym zakresie.
 - 4) **zdolności technicznej lub zawodowej:**
Zamawiający nie stawia warunku w powyższym zakresie.

PODSTAWY WYKLUCZENIA

1. Z postępowania o udzielenie zamówienia wyklucza się Wykonawców, w stosunku do których zachodzi którakolwiek z okoliczności wskazanych:
 - 1) Zamawiający wykluczy z postępowania Wykonawcę w przypadkach określonych w art. 108 ust. 1 ustawy Pzp, tj. Wykonawcę:
 - a) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
 - udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
 - handlu ludźmi, o którym mowa w art. 189 a Kodeksu karnego,
 - o którym mowa w art. 228-230 a, art. 250 a Kodeksu karnego lub w art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie,
 - finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
 - o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
 - powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. 2021r., poz. 1745),
 - przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,
 - o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

- b) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;
 - c) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
 - d) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
 - e) jeżeli Zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi Wykonawcami porozumienie mające na celu zaskócenie konkurencji, w szczególności, jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;
 - f) jeżeli, w przypadkach, o których mowa w art. 85 ust. 1 ustawy Pzp, doszło do zaskócenia konkurencji wynikającego z wcześniejszego zaangażowania tego Wykonawcy lub podmiotu, który należy z Wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zaskócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie Wykonawcy z udziału w postępowaniu o udzielenie zamówienia.
- 2) Zamawiający wykluczy z postępowania także Wykonawcę w przypadkach określonych w art. 109 ust. 1 ustawy Pzp:
- a) pkt 4 - 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,
 - b) pkt 5 – który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności, gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienia, co zamawiający jest w stanie wykazać za pomocą stosownych dowodów,
 - c) pkt 7 – który z przyczyn leżących po jego stronie, w znacznym stopniu lub zakresie nie wykonał lub nienależycie wykonał albo długotrwale nienależycie wykonał, istotne zobowiązanie wynikające z wcześniejszej umowy w sprawie zamówienia publicznego lub umowy koncesji, co doprowadziło do wypowiedzenia umowy lub odstąpienia od umowy, odszkodowania, wykonania zastępczego lub realizacji uprawnień z tytułu rękojmi za wady.
2. Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania. Wykluczenie Wykonawcy następuje zgodnie z art. 111 ustawy Pzp, z zastrzeżeniem art. 110 ust. 2 i 3 ustawy Pzp.
3. Zgodnie z zapisami art. 1 pkt 3) oraz art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. poz. 835) z postępowania wyklucza się:
- 1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3;
 - 2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została

wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3;

- 3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120) 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.

ROZDZIAŁ 9.

OŚWIADCZENIA I DOKUMENTY, JAKIE ZOBOWIĄZANI SĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ WYKAZANIA BRAKU PODSTAW WYKLUCZENIA (PODMIOTOWE ŚRODKI DOWODOWE)

1. Do Formularza ofertowego Wykonawca zobowiązany jest na podstawie art. 125 ust. 1 ustawy PZP dołączyć aktualne na dzień składania ofert oświadczenie, zgodne z wzorem stanowiącym Załącznik nr 2 do SWZ, stanowiące wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu.
2. Zamawiający wymaga od Wykonawców złożenia wraz z Formularzem ofertowym Załącznika nr 1 na poświadczenie zapoznania się z warunkami zawartymi w SWZ.
3. Informacje zawarte w oświadczeniu, o którym mowa w ust. 1 stanowią wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu.
4. W przypadku wspólnego ubiegania się o zamówienie przez wykonawców, oświadczenie, o którym mowa w ust. 1, składa każdy z Wykonawców.
5. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia, wraz z oświadczeniem, o którym mowa w ust. 1, także oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu.
6. Jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, Zamawiający może na każdym etapie postępowania, w tym na etapie składania wniosków o dopuszczenie do udziału w postępowaniu lub niezwłocznie po ich złożeniu, wezwać Wykonawców do złożenia wszystkich lub niektórych podmiotowych środków dowodowych aktualnych na dzień ich złożenia. Jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio podmiotowe środki dowodowe nie są już aktualne, Zamawiający może w każdym czasie wezwać Wykonawcę lub Wykonawców do złożenia wszystkich lub niektórych podmiotowych środków dowodowych aktualnych na dzień ich złożenia.
7. Na wezwanie Zamawiającego Wykonawca zobowiązany jest do złożenia następujących oświadczeń lub dokumentów potwierdzających brak podstaw wykluczenia:
 - 1) odpis lub informacja z Krajowego Rejestru Sądowego lub Centralnej Ewidencji i Informacji o Działalności Gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji – w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 109 ust. 1 pkt. 4 ustawy Pzp; (Na podstawie art. 127 ust. 1 pkt 1 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 jednolitym dokumencie dane umożliwiające dostęp do tych środków).
 - 2) oświadczenie Wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy Pzp, 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 2024 r. poz. 594), z innym Wykonawcą, który złożył odrębną ofertę, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami

potwierdzającymi przygotowanie oferty niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej.

- 3) oświadczenie Wykonawcy w zakresie art. 108 ust. 1 pkt 3 ustawy Pzp, o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne albo — w przypadku wydania takiego wyroku lub decyzji dokumentów potwierdzających dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności - **załącznik nr 9 do SWZ**;
- 4) oświadczenie Wykonawcy w zakresie określonym w art. 108 ust. 1 pkt 4 ustawy PZP o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienie publiczne - **załącznik nr 9 do SWZ**.

Zamawiający w sytuacji, gdy wykonawca polega na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 118 ustawy PZP żąda przedstawienia w odniesieniu do tych podmiotów dokumentów wymienionych powyżej.

8. Dokumenty podmiotów zagranicznych:

1) Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentów, o których mowa w pkt 7:

- a) ppkt 1— zamiast odpisu lub informacji z Krajowego Rejestru Sądowego lub Centralnej Ewidencji i Informacji o Działalności Gospodarczej, składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że: 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,
- b) ppkt 2 — zamiast informacji z Krajowego Rejestru Karnego, składa informację z odpowiedniego rejestru, takiego jak rejestr sądowy albo w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, w zakresie określonym w art. w art. 108 ust. 1 pkt 1, 2 i 4 ustawy.

2) Dokumenty, o których mowa:

- w pkt 8 ust. 1 ppkt a) powinny być wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu;
- w pkt 8 ust. 1 ppkt b) powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu.

3) Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w ust. 1, lub gdy dokumenty te nie odnoszą się do wszystkich przypadków, o których mowa w art. 108 ust. 1 pkt 1, 2 i 4, art. 109 ust. 1 pkt 1, 2 lit. a i b oraz pkt 3 ustawy Pzp, 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.

4) W przypadku wątpliwości co do treści dokumentu złożonego przez Wykonawcę, Zamawiający może zwrócić się do właściwych organów odpowiednio kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, o udzielenie niezbędnych informacji dotyczących tego dokumentu.

- 5) Dokumenty te są składane w formie oryginału lub kopii poświadczonych za zgodność z oryginałem przez Wykonawcę wraz z tłumaczeniem na język polski.
9. Podmiotowe środki dowodowe, przedmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski. W przypadku wskazania przez Wykonawcę dostępności podmiotowych środków dowodowych pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych, Zamawiający żąda od Wykonawcy przedstawienia tłumaczenia na język polski pobranych samodzielnie przez Zamawiającego podmiotowych środków dowodowych.
10. Podmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, o których mowa powyżej, składa się w formie elektronicznej (z kwalifikowanym podpisem elektronicznym), w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym. Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgodny z wymaganiami określonymi w Rozporządzeniu PRM.
11. 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 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile Wykonawca wskazał w oświadczeniu, o którym mowa w art. 125 ust.1 ustawy Pzp dane umożliwiające dostęp do tych środków.
12. Jeżeli Wykonawca nie złożył oświadczenia, o którym mowa w pkt 1, podmiotowych środków dowodowych, przedmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu lub są one niekompletne lub zawierają błędy, Zamawiający wzywa wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w wyznaczonym terminie, chyba że oferta Wykonawcy podlega odrzuceniu bez względu na ich złożenie, uzupełnienie lub poprawienie lub zachodzą przestanki unieważnienia postępowania.
13. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które Zamawiający posiada, jeżeli Wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.

ROZDZIAŁ 10.

INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ LUB DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI

1. W postępowaniu o udzielenie zamówienia publicznego komunikacja między Zamawiającym a wykonawcami odbywa się przy użyciu Platformy zakupowej OPEN NEXUS.
- Zamawiający na podstawie art. 65 ust. 1 pkt 4 ustawy Pzp odstępuje od wymagania użycia środków komunikacji elektronicznej w zakresie części oferty – próbki oprogramowania, stanowiącej przedmiotowy środek dowodowy. W związku z powyższym, na podstawie art. 65 ust. 2 ustawy Pzp, Zamawiający wymaga, aby w/w próbka, przygotowana zgodnie z wytycznymi zawartymi w Załączniku nr 10 do SWZ, została przekazana:
- a) za pośrednictwem operatora pocztowego w rozumieniu ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (t.j. Dz.U. 2020, poz. 1041 i 2320) lub
 - b) osobiście lub
 - c) za pośrednictwem postańca,
- na adres Zamawiającego wskazany w Rozdziale 1 SWZ, przed upływem terminu składania ofert, w kopercie opatrzonej nazwą i adresem Wykonawcy, nazwą i numerem referencyjnym postępowania oraz adnotacją, że koperta zawiera przedmiotowe środki dowodowe tj. próbkę oprogramowania. Niezależnie od powyższego

pozostałe dokumenty składające się na ofertę, zgodnie z art. 65 ust. 3 ustawy Pzp, Wykonawca przedkłada w formie elektronicznej.

2. Korzystanie z Platformy zakupowej OPEN NEXUS jest bezpłatne.
3. Adres strony internetowej prowadzonego postępowania (link prowadzący bezpośrednio do widoku postępowania na Platformie e-Zamówienia): <https://platformazakupowa.pl/transakcja/1082177>
4. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym, a Wykonawcami w szczególności zadawanie pytań, umieszczanie zawiadomień oraz przekazywanie informacji odbywa się drogą elektroniczną za pośrednictwem formularza "Wyślij wiadomość" dostępnego na stronie publikowanego postępowania za pośrednictwem platformy zakupowej OPEN NEXUS.
5. Przeglądanie i pobieranie publicznej treści dokumentacji postępowania nie wymaga posiadania konta na Platformie zakupowej ani logowania.
6. Wykonawca przystępując do niniejszego postępowania o udzielenie zamówienia publicznego, akceptuje warunki korzystania z platformy zakupowej OPEN NEXUS, określone w regulaminie portalu dostępnym pod adresem: <https://platformazakupowa.pl/strona/1-regulamin>.
7. Wymagania techniczne i organizacyjne wysyłania i odbierania korespondencji elektronicznej przekazywanej przy ich użyciu, opisane zostały w regulaminie portalu dostępnym pod w/w adresem.
8. Występuje limit objętości plików lub spakowanych folderów w zakresie całej oferty lub wniosku do 1 GB przy maksymalnej ilości 20 plików lub spakowanych folderów.
9. W przypadku większych plików zalecamy skorzystać z instrukcji pakowania plików opracowanej przez platformę zakupową OPEN NEXUS, dzieląc je na mniejsze paczki po np. 75 MB każda – link do instrukcji: https://docs.google.com/document/d/1kdC7je8RNO5FSk_N0NY7nv1Xj1WYJza-CmXvYH8evhk/edit.
10. Zamawiający dopuszcza przesyłanie danych w formatach dopuszczonych odpowiednimi przepisami prawa, tj. m.in.: .doc, .docx, .txt, .xls, .xlsx, .ppt, .csv, .pdf, .jpg, .git, .png, .tif, .dwg, .ath, .kst, .zip, .rar, przy czym zaleca się wykorzystywanie plików w formacie .pdf.
11. Za datę przekazania oświadczeń, wniosków, zawiadomień, dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń oraz innych informacji przyjmuje się datę ich doręczenia za pośrednictwem formularza "Wyślij wiadomość" dostępnego na stronie danego postępowania.
12. Sposób sporządzenia dokumentów elektronicznych lub dokumentów elektronicznych będących kopią elektroniczną treści zapisanej w postaci papierowej (cyfrowe odwzorowania) musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych.
13. Dokumenty elektroniczne, o których mowa w § 2 ust. 1 rozporządzenia Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych, sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, z uwzględnieniem rodzaju przekazywanych danych i przekazuje się jako załączniki.
W przypadku formatów, o których mowa w art. 66 ust. 1 ustawy Pzp, ww. regulacje nie będą miały bezpośredniego zastosowania.
14. Informacje, oświadczenia lub dokumenty, inne niż wymienione w § 2 ust. 1 rozporządzenia Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych, przekazywane w postępowaniu sporządza się w postaci elektronicznej:
 - a) w formatach danych określonych w przepisach rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (i przekazuje się jako załącznik), lub
 - b) jako tekst wpisany bezpośrednio do wiadomości przekazywanej przy użyciu środków komunikacji elektronicznej (np. w treści wiadomości e-mail lub w treści „Formularza do komunikacji”).
15. Jeżeli dokumenty elektroniczne, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233) wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem w nazwie pliku „Dokument stanowiący tajemnicę przedsiębiorstwa”.

16. Zamawiający dopuszcza również komunikację elektroniczną (inną niż oferta Wykonawcy i załączniki do oferty) za pomocą poczty elektronicznej, adres poczty elektronicznej: zam.publiczne@wielkanieszawka.pl.
17. Zamawiający nie przewiduje sposobu komunikowania się z Wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej, wskazanych w SWZ.
18. Postępowanie o udzielenie zamówienia prowadzi się w języku polskim.
19. W korespondencji kierowanej do Zamawiającego Wykonawcy powinni posługiwać się numerem przedmiotowego postępowania.

ROZDZIAŁ 11. WYJAŚNIENIA TREŚCI SWZ

1. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ:
 - 1) 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 odpowiednio SWZ wpłynął do zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert;
 - 2) Jeżeli wniosek o wyjaśnienie treści specyfikacji istotnych warunków zamówienia wpłynął po upływie ww. terminu składania wniosku lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień lub pozostawić wniosek bez rozpoznania.
2. W uzasadnionych przypadkach na zasadach określonych w ustawie Pzp Zamawiający może zmienić treść SWZ. Dokonana w ten sposób zmiana zostanie udostępniona na stronie internetowej Zamawiającego.
3. Zamawiający nie przewiduje zwołania zebrania Wykonawców.
4. Zamawiający nie przewiduje sposobu komunikowania się z Wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej, wskazanych w SWZ.

ROZDZIAŁ 12. OPIS SPOSOBU PRZYGOTOWANIA OFERT

1. Oferta musi być sporządzona w języku polskim, w postaci elektronicznej i opatrzona kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
2. Do przygotowania oferty konieczne jest posiadanie przez osobę upoważnioną do reprezentowania Wykonawcy kwalifikowanego podpisu elektronicznego, podpisu osobistego lub podpisu zaufanego.
3. Do przygotowania oferty zaleca się wykorzystanie formularza ofertowego, którego wzór Zamawiający zamieścił na stronie internetowej prowadzonego postępowania. W przypadku, gdy Wykonawca nie korzysta z przygotowanego przez Zamawiającego wzoru, w treści oferty należy zamieścić wszystkie informacje wymagane w formularzu ofertowym.
4. Oferta składana za pośrednictwem platformy zakupowej OPEN NEXUS, w sposób automatyczny zostaje zaszyfrowana. Pliki Oferty wraz z załącznikami załączone przez Wykonawcę na platformie zakupowej stają się dokumentami zaszyfrowanymi.
5. Możliwość otwarcia plików dostępna jest dopiero po odszyfrowaniu plików przez Zamawiającego po upływie terminu otwarcia ofert.
6. Z uwagi na to, że oferta wykonawcy jest zaszyfrowana, nie można jej edytować. Przez zmianę oferty rozumie się złożenie nowej oferty i wycofanie poprzedniej, jednak należy to zrobić przed upływem terminu zakończenia składania ofert w postępowaniu.

7. Złożenie nowej oferty lub wniosku i wycofanie poprzedniej w postępowaniu w którym zamawiający dopuszcza złożenie tylko jednej oferty lub wniosku przed upływem terminu zakończenia składania ofert w postępowaniu powoduje wycofanie oferty poprzednio złożonej.
8. Jeśli wykonawca składający ofertę lub wniosek jest zautoryzowany (zalogowany), to wycofanie oferty lub wniosku następuje od razu po złożeniu nowej oferty.
9. Jeżeli oferta lub wniosek składana jest przez niezautoryzowanego wykonawcę (niezalogowany lub nieposiadający konta) to wycofanie oferty musi być przez niego potwierdzone:
 - 1) przez kliknięcie w link wysłany w wiadomości email, który musi być zgodny z adres e-mail podanym podczas pierwotnego składania oferty lub
 - 2) zalogowanie i kliknięcie w przycisk Potwierdź ofertę.
10. Potwierdzeniem wycofania oferty lub wniosku w przypadku kliknięcia w link jest data kliknięcia w przycisk Wycofaj ofertę i potwierdzenie tej akcji.
11. Wycofanie oferty lub wniosku możliwe jest do zakończenia terminu składania ofert lub wniosków w postępowaniu.
12. Wycofanie złożonej oferty powoduje, że zamawiający nie będzie miał możliwości zapoznania się z nią po upływie terminu zakończenia składania ofert w postępowaniu.
13. Wykonawca po upływie terminu składania ofert nie może dokonać zmiany złożonej oferty lub wniosku.
14. Wykonawca może złożyć ofertę lub wniosek po terminie składania ofert lub wniosku poprzez kliknięcie przycisku Odblokuj formularz.
15. W przypadku złożenia oferty po terminie wykonawca otrzymuje automatyczny komunikat dotyczący tego, że oferta została złożona po terminie.
16. Zamawiający informuje, że oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r., poz. 1233 z późn. zm.), jeśli Wykonawca w terminie składania ofert zastrzegł, że nie mogą one być udostępniane i jednocześnie wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
17. Zamawiający zaleca, aby informacje zastrzeżone, jako tajemnica przedsiębiorstwa były przez Wykonawcę złożone w odrębnym pliku z opisem „Tajemnica przedsiębiorstwa”. Wykonawca zobowiązany jest, wraz z przekazywaniem tych informacji, wykazać spełnienie przesłanek określonych w art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r., poz. 1233 z późn. zm.). Zastrzeżenie przez Wykonawcę tajemnicy przedsiębiorstwa bez uzasadnienia, będzie traktowane przez Zamawiającego jako bezskuteczne ze względu na zaniechanie przez Wykonawcę podjęcia niezbędnych działań w celu zachowania poufności objętych klauzulą informacji zgodnie z postanowieniami art. 18 ust. 3 Pzp.
18. Brak jednoznacznego wskazania, które informacje stanowią tajemnicę przedsiębiorstwa oznaczać będzie, że wszelkie oświadczenia i zaświadczenia składane w trakcie niniejszego postępowania są jawne bez zastrzeżeń.

OFERTA SKŁADA SIĘ Z:

- 1) Formularza oferty sporządzonego według wzoru stanowiącego Załącznik nr 1 do SWZ;
- 2) Oświadczenia, o którym mowa w art.125 ust. 1 ustawy Pzp - Załącznik nr 2 do SWZ;
- 3) *zobowiązania podmiotu udostępniającego zasoby lub inny podmiotowy środek dowodowy, o którym mowa w rozdziale 6 SWZ – załącznik nr 6 do SWZ (jeżeli dotyczy);*
- 4) *pełnomocnictwa lub innego dokumentu potwierdzającego umocowanie do reprezentowania Wykonawcy dla osoby/osób podpisującej/cych ofertę zgodnie z rozdziału 7 ust. 1 SWZ (jeżeli dotyczy);*
- 5) *W przypadku, gdy oferta zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233), Wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku – szczegóły opisane rozdziale 12 ust. 10 SWZ (jeżeli dotyczy);*
- 6) Przedmiotowego środka dowodowego w postaci próbki oprogramowania

- 7) Wraz z ofertą nie należy składać dokumentów podmiotowych środków dowodowych. Dokumenty te składa Wykonawca, którego oferta została najwyżej oceniona, po otrzymaniu wezwania Zamawiającego;
- 8) Środki dowodowe lub inne dokumenty, w tym dokumenty potwierdzające umocowanie do reprezentowania, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski.

ROZDZIAŁ 13. WADIUM

1. Zamawiający nie wymaga wniesienia wadium.

ROZDZIAŁ 14. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca będzie związany złożoną ofertą przez 30 dni, tj. do dnia **3 maja 2025 roku**.
2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
3. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą wskazanego w ust. 1, Zamawiający przed upływem terminu związania ofertą zwraca się jednokrotnie do wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni. Przedłużenie terminu związania ofertą wymaga złożenia przez wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

ROZDZIAŁ 15. MIEJSCE I TERMIN SKŁADANIA I OTWARCIA OFERT

1. Ofertę należy złożyć poprzez platformę zakupową OPEN NEXUS (z zastrzeżeniem dotyczącym sposobu przekazania przedmiotowego środka dowodowego, tj. próbki oferowanego oprogramowania) do dnia **4 kwietnia 2025 do godz. 10:00**
2. Za datę złożenia oferty rozumie się datę jej wpływu na Platformę, za wyjątkiem próbki, o terminie złożenia której decyduje data i godzina jej wpływu do siedziby Zamawiającego, na adres wskazany w Rozdziale 1 SWZ.
3. Oferty zgodnie z art. 63 ust 2 ustawy PZP winny być złożone pod rygorem nieważności w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym (w postaci elektronicznej opatrzonej podpisem zaufanym, o którym mowa w ustawie z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307) lub podpisem osobistym, o którym mowa w ustawie z 6.08.2010 r. o dowodach osobistych (Dz. U. z 2022 r. poz. 671).
4. Warunki zachowania elektronicznej formy są określone w art. 781 ustawy z 23.04.1964 r. – Kodeks cywilny (Dz. U. z 2024 r. poz. 1061) – dalej k.c. Zgodnie z tym przepisem do zachowania elektronicznej formy czynności prawnej wystarcza złożenie oświadczenia woli w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym.
5. Zgodnie zaś z treścią art. 99 § 1 k.c., jeżeli do ważności czynności prawnej potrzebna jest szczególna forma, pełnomocnictwo do dokonania tej czynności powinno być udzielone w tej samej formie. Przepisy ustawy pzp ustanawiają rygor nieważności dla złożenia oferty w inny sposób niż wskazany w jej przepisach. Jeśli więc wykonawca jest zobowiązany do złożenia oferty w formie elektronicznej (podpisanej kwalifikowanym

podpisem elektronicznym), lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym, to pełnomocnictwo do podpisania oferty winno być złożone w tej samej formie.

6. Otwarcie ofert nastąpi w dniu **4 kwietnia 2025 roku o godz. 10:30**. Zamawiający nie przewiduje jawnej sesji otwarcia ofert.
7. Najpóźniej przed otwarciem ofert, udostępnia się na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza się przeznaczyć na sfinansowanie zamówienia.
8. Niezwłocznie po otwarciu ofert, udostępnia się na stronie internetowej prowadzonego postępowania informacje o:
 - 1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
 - 2) cenach lub kosztach zawartych w ofertach.

ROZDZIAŁ 16. SPOSÓB OBLICZANIA CENY

1. Zamawiający informuje, że za wykonanie przedmiotu zamówienia określonego w niniejszej SWZ, ustala się wynagrodzenie ryczałtowe.
2. Cenę całkowitą należy podać w złotych z dokładnością do dwóch miejsc po przecinku. Zamawiający nie przewiduje rozliczeń w walutach obcych.
3. Cena oferty obejmować musi wszelkie wymagania Zamawiającego i czynności związane z wykonaniem zamówienia, w tym wszelkie koszty, jakie poniesie Wykonawca z tytułu należytej realizacji przedmiotu zamówienia, zgodnej z warunkami, o których mowa w SWZ i załącznikach do SWZ oraz właściwą stawkę podatku VAT od towarów i usług dla przedmiotu zamówienia.
4. Cena ofertowa musi zawierać wszystkie koszty niezbędne do zrealizowania zamówienia wynikające wprost z koncepcji i prawnej, jak również w niej nieujęte, a bez których nie można wykonać zamówienia, w tym koszty wynikające z obowiązków wykonawcy określonych w przedmiocie zamówienia.
5. W toku badania i oceny ofert Zamawiający może żądać wyjaśnień dotyczących treści złożonych ofert. Nie dopuszcza się prowadzenia między Zamawiającym a Wykonawcą negocjacji dotyczących złożonej oferty.
6. Zamawiający zwróci się o udzielenie wyjaśnień, w tym o złożenie dowodów, dotyczących elementów oferty mających wpływ na wysokość ceny, jeżeli zaoferowana cena oferty lub jej istotne części składowe wydawać się będą rażąco niskie w stosunku do przedmiotu zamówienia i budzić będą wątpliwości Zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi przez Zamawiającego lub wynikającymi z odrębnych przepisów. Sytuacja ta ma miejsce w szczególności, gdy zaoferowana przez Wykonawcę cena oferty jest niższa o 30% od wartości zamówienia powiększonej o należny podatek VAT od towarów i usług lub średniej arytmetycznej cen wszystkich złożonych ofert.
7. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu spoczywa na wykonawcy.
8. Zamawiający odrzuca ofertę Wykonawcy, który nie udzielił wyjaśnień, o których mowa w ust. 6 lub jeżeli dokonana ocena wyjaśnień oraz złożonych przez Wykonawcę dowodów potwierdza, że złożona oferta zawiera rażąco niską cenę lub koszt w stosunku do przedmiotu zamówienia.
9. Faktury opłacone będą – przelewem na rachunek Wykonawcy. Za datę płatności uważa się datę wydania przez Zamawiającego polecenia przelewu pieniędzy. Faktury opłacane będą w terminie 30 dni od daty dostarczenia ich Zamawiającemu.

ROZDZIAŁ 17.

SPOSÓB OCENY KRYTERIÓW WYBORU OFERTY

1. Przy dokonywaniu wyboru najkorzystniejszej oferty Zamawiający stosować będzie następujące kryteria oceny ofert [dla Części I-V]:

Lp.	Kryterium	Znaczenie procentowe kryterium	Maksymalna ilość punktów jakie może otrzymać oferta za dane kryterium
1.	Cena – C	60%	60
2.	Termin realizacji – D*	40%	40

* dot. części I, części II etap I, części III etap I, części IV etap I, części V,

2. Za najkorzystniejszą ofertę zostanie uznana oferta, która otrzyma największą sumę punktów wyliczonych według powyższych wzorów i zasad. Wszystkie wyniki zostaną przez Zamawiającego zaokrąglone, zgodnie z zasadami matematycznymi, z dokładnością do dwóch miejsc po przecinku.

$$O = C + D$$

gdzie:

O - całkowita liczba punktów przyznanych ofercie,

C - liczba punktów przyznanych za kryterium 1 – Cena,

D - liczba punktów przyznanych za kryterium 2 – Termin realizacji

3. Zasady oceny:

- a) w kryterium „Cena” zastosowany zostanie następujący wzór arytmetyczny, gdzie „C” oznacza otrzymaną przez Wykonawcę liczbę punktów (maksymalna liczba punktów – 60):

$$C = \frac{\text{najniższa cena brutto}}{\text{cena brutto oferty ocenianej}} \times 60$$

- b) punkty za kryterium „Termin realizacji” przyznane Wykonawcy na podstawie oświadczenia dotyczącego skrócenia terminu dostawy zawartego w formularzu oferty.

Termin realizacji	Ilość punktów
Brak skrócenia terminu realizacji	0
Skrócenie terminu realizacji o 30 dni	40

4. Jeżeli nie można wybrać oferty najkorzystniejszej z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający spośród tych ofert wybiera ofertę z najniższą ceną, a jeżeli zostały złożone oferty o takiej samej cenie, Zamawiający wzywa Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych.
5. Wykonawcy, składając oferty dodatkowe, nie mogą zaoferować cen wyższych niż zaoferowane w złożonych ofertach.

ROZDZIAŁ 18.

FORMALNOŚCI, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY

1. Zamawiający skontaktuje się z wybranym Wykonawcą, w celu uzgodnienia szczegółów zawarcia Umowy, a także innych kwestii związanych ze sprawnym jej zawarciem.
2. Umowa zostanie zawarta z wybranym Wykonawcą w terminach określonych w art. 308 ust. 2 Pzp.
3. Wykonawca, któremu przyznane zostanie wykonanie zamówienia publicznego zobowiązany jest przed podpisaniem umowy do:
 - a) w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, których oferta została wybrana jako oferta najkorzystniejsza, zawarcia i przedłożenia umowy regulującej zasady ich współpracy.
4. Wybrany Wykonawca ma obowiązek zawrzeć Umowę, której ogólne warunki określono we wzorze Umowy.

ROZDZIAŁ 19.

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

1. Jako odrębny Załącznik nr 7 do SWZ Zamawiający zamieści wzór umowy, który określa warunki realizacji przedmiotu zamówienia.
2. Zamawiający przewiduje możliwość zmiany zawartej umowy w stosunku do treści wybranej oferty w zakresie uregulowanym w art. 454-455 ustawy Pzp oraz wskazanym we wzorze umowy.

ROZDZIAŁ 20.

ŚRODKI OCHRONY PRAWNEJ

1. Środki ochrony prawnej przysługują w okolicznościach i na zasadach określonych w dziale IX ustawy prawo zamówień publicznych.
2. Środki ochrony prawnej przysługują wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy Pzp.
3. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub ogłoszenia o konkursie oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 Pzp, oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
4. Odwołanie przysuguje na:
 - 1) niezgodną z przepisami ustawy czynność zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, o zawarcie umowy ramowej, dynamicznym systemie zakupów, systemie kwalifikowania wykonawców lub konkursie, w tym na projektowane postanowienie umowy;
 - 2) zaniechanie czynności w postępowaniu o udzielenie zamówienia, o zawarcie umowy ramowej, dynamicznym systemie zakupów, systemie kwalifikowania wykonawców lub konkursie, do której zamawiający był obowiązany na podstawie ustawy;
 - 3) zaniechanie przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy, mimo że zamawiający był do tego obowiązany.

5. Odwołanie wnosi się do Prezesa Izby.
6. Odwołujący przekazuje zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on się zapoznać z jego treścią przed upływem tego terminu. Domniemywa się, iż zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przekazanie odpowiednio odwołania lub jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
7. Odwołanie wnosi się w terminach określonych w art. 515 ustawy Pzp.
8. Na orzeczenie Izby oraz postanowienie Prezesa Izby, o którym mowa w art. 519 ust. 1 ustawy pzp, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.
9. Skargę wnosi się do Sądu Okręgowego w Warszawie - sądu zamówień publicznych, zwanego dalej "sądem zamówień publicznych".
10. Skargę wnosi się za pośrednictwem Prezesa Izby, w terminie 14 dni od dnia doręczenia orzeczenia Izby lub postanowienia Prezesa Izby, o którym mowa w art. 519 ust. 1 pzp, przesyłając jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora wyznaczonego w rozumieniu ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe jest równoznaczne z jej wniesieniem.
11. Prezes Izby przekazuje skargę wraz z aktami postępowania odwoławczego do sądu zamówień publicznych w terminie 7 dni od dnia jej otrzymania.

ROZDZIAŁ 21. POSTANOWIENIA KOŃCOWE

1. W sprawach nieuregulowanych w niniejszej specyfikacji mają zastosowanie przepisy ustawy Prawo Zamówień Publicznych oraz przepisy Kodeksu Cywilnego.
2. Wszystkie załączniki do niniejszej SWZ stanowią jej integralną część.

ZAŁĄCZNIKI DO SWZ:

1. Formularz Oferty: **Załącznik nr 1;**
2. Oświadczenie o braku podstaw do wykluczenia: **Załącznik nr 2;**
3. Oświadczenie dotyczące przynależności lub braku przynależności do tej samej grupy kapitałowej: **Załącznik nr 3;**
4. Zobowiązanie podmiotu trzeciego: **Załącznik nr 6;**
5. Wzór Umowy: **Załącznik nr 7;**
6. Oświadczenie wykonawców wspólnie ubiegających się o udzielenie zamówienia – **załącznik nr 8;**
7. Oświadczenie Wykonawcy – **Załącznik nr 9.**
8. Wymagania dotyczące próbki przedmiotu zamówienia oraz zasady i zakres jej badania – **Załącznik nr 10.**

FORMULARZ OFERTY

Nazwa Wykonawcy:

NIP:

REGON:

Miejscowość:

Kod pocztowy:

Kraj:

Adres pocztowy (ulica, nr domu i lokalu):

Województwo:

E-mail:

Tel.:

Adres internetowy (URL):

Osoba upoważniona do kontaktu z Zamawiającym:

Składając ofertę w postępowaniu na **Dostawa sprzętu, oprogramowania oraz usług informatycznych**
– nr ref.: **RIT.271.2.4.2025.MR**

1. Oferujemy wykonanie przedmiotu zamówienia za łączną ryczałtową cenę w zakresie CZĘŚCI:
netto zł.

powiększoną o podatek VAT %,

co daje cenę brutto zł

(słownie złotych:),

[powielić odpowiednio, w zależności od ilości części, na które składana jest oferta]

w tym:

Lp.	Rodzaj	Ilość	Proponowany model / producent	Cena jednostkowa netto [PLN]	Wartość netto [PLN]	Podatek Vat [%]	Wartość brutto [PLN]
CZĘŚĆ I							
	URZĄD GMINY W WIELKIEJ NIESZAWCE						
1.	UTM Zapora sieciowa	1					
RAZEM CZĘŚĆ I:							

CZĘŚĆ II

ETAP I

GMINNY OŚRODEK POMOCY SPOŁECZNEJ							
1.	Zasilacz awaryjny – UPS 850VA	5 szt.					
2.	Zasilacz awaryjny – UPS 1200VA	1 szt.					
ETAP II							
URZĄD GMINY W WIELKIEJ NIESZAWCE							
1.	Zasilacz awaryjny – UPS 850VA	16 szt.					
2.	Zasilacz awaryjny – UPS 1600VA	1 szt.					
RAZEM CZĘŚĆ II:							

CZĘŚĆ III							
ETAP I							
GMINNY OŚRODEK POMOCY SPOŁECZNEJ							
1.	Serwer 1	1 szt.					
2.	Serwer 2	1 szt.					
3.	Oprogramowanie oraz monitoring usług i użytkowanych systemów	1 szt.					
ETAP II							
URZĄD GMINY W WIELKIEJ NIESZAWCE							
1.	System umożliwiający monitoring komputerów	1 szt.					
2.	Oprogramowanie oraz monitoring usług i użytkowanych systemów	1 szt.					
RAZEM CZĘŚĆ III:							

CZĘŚĆ IV							
ETAP I							
GMINNY OŚRODEK POMOCY SPOŁECZNEJ							
1.	Usługa chmurowa dla backup baz danych	1 szt.					
ETAP II							
URZĄD GMINY W WIELKIEJ NIESZAWCE							
1.	Usługa chmurowa dla backup baz danych	1 szt.					
RAZEM CZĘŚĆ IV:							

CZĘŚĆ V							
URZĄD GMINY W WIELKIEJ NIESZAWCE							

1.	System backup	1 szt.					
2.	Punkty dostępowe	2 szt.					
RAZEM CZĘŚĆ V:							

2. Podana cena uwzględnia wszystkie koszty związane z realizacją przedmiotu zamówienia określonego w SWZ wraz z załącznikami.
3. Oświadczamy, że oferujemy skrócenie terminu realizacji o:

Skrócenie terminu realizacji dla CZĘŚCI / ETAPU I*	
0 dni	☐
30 dni	☐

*uzupełnić w zależności od części, na którą składana jest oferta

4. Oświadczamy, że zapoznaliśmy się z opisem przedmiotu zamówienia i nie wnosimy do niego żadnych zastrzeżeń, a oferowany przez nas przedmiot zamówienia jest zgodny ze wszystkimi jego wymaganiami.
5. Oświadczamy, że zapoznaliśmy się z SWZ wraz z załącznikami i nie wnosimy do niej zastrzeżeń oraz zdobyliśmy wszystkie niezbędne informacje do przygotowania oferty.
6. Oświadczamy, że zawarty w SWZ wzór umowy został przez nas zaakceptowany i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy na warunkach wskazanych we wzorze umowy stanowiącym Załącznik do SWZ, w miejscu i terminie wskazanym przez Zamawiającego.
7. Niniejszym potwierdzamy, że pozostajemy związani niniejszą ofertą do dnia wskazanego w SWZ.
8. Oświadczamy, że¹:
- ☐ wybór naszej oferty nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług.
- ☐ wybór naszej oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług. Wykonawca w związku z tym wskazuje:
- nazwę (rodzaju) towaru, którego dostawa będzie prowadziła do powstania obowiązku podatkowego: _____
 - wartości towaru objętego obowiązkiem podatkowym Zamawiającego, bez kwoty podatku: _____
 - stawkę podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie: _____
9. Oświadczamy, że jesteśmy²:
- ☐ mikroprzedsiębiorstwem
- ☐ małym przedsiębiorstwem
- ☐ średnim przedsiębiorstwem
- ☐ jednoosobowa działalność gospodarcza
- ☐ osoba fizyczna nieprowadząca działalności gospodarczej
- ☐ inny rodzaj

10. Oświadczamy, że informacje zawarte w ofercie, w następującym zakresie: _____³ stanowią tajemnicę

przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji (t.j. Dz.U. 2020, poz. 1913 ze zm.) i jako takie nie mogą być udostępniane innym uczestnikom postępowania (w przypadku zastrzeżenia informacji przez Wykonawcę zobowiązany jest on, wraz z ich przekazaniem, wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa).

11. przedmiot zamówienia wykonamy siłami własnymi / przy udziale podwykonawców*, którym zamierzamy powierzyć wykonanie następujących części zamówienia i podajemy firmy/nazwy podwykonawców:

L.P.	CZĘŚĆ/ZAKRES ZAMÓWIENIA	NAZWA PODWYKONAWCY
1		
2		

(*) niepotrzebne skreślić

12. Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO⁴ wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.⁶

13. Do oferty załączamy następujące dokumenty:

- 1) _____
2) _____

^{1.} Zaznaczyć właściwe i jeśli dotyczy – uzupełnić wymagane informacje

^{2.} Zaznaczyć właściwe / ta informacja jest wymagana wyłącznie do celów statystycznych

Zgodnie z zaleceniem Komisji z dnia 6 maja 2003r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz. U. L124 z 20.5.2003 s.36):

- mikroprzedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2.000.000,00 EURO
- małe przedsiębiorstwo - przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10.000.000,00 EURO.
- średnie przedsiębiorstwo: przedsiębiorstwo, które nie jest mikroprzedsiębiorstwem ani małym przedsiębiorstwem i które zatrudnia mniej niż 250 osób i którego roczny obrót nie przekracza 50.000.000,00EURO lub roczna suma bilansowa nie przekracza 43.000.000.00EURO

W sytuacji składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia – zapis odpowiednio powielić lub wskazać dane tylko w odniesieniu do pełnomocnika.

- ^{3.} Wskazać zakres informacji stanowiących tajemnicę przedsiębiorstwa i przedłożyć stosowne uzasadnienie zastrzeżenia tych informacji
- ^{4.} Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1)
- ^{5.} W przypadku gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie składa (przez jego wykreślenie)

Wykonawca:

(nazwa firmy oraz adres wykonawcy)

(NIP, REGON, KRS)

(nr tel, adres e-mail)

**Oświadczenie wykonawcy/wykonawcy wspólnie ubiegającego się o zamówienie/ podmiotu
udostępniającego zasoby*
składane na podstawie art. 125 ust. 1 ustawy Pzp**

O NIEPODLEGANIU WYKLUCZENIU

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

Na potrzeby postępowania o udzielenie zamówienia publicznego oświadczam, co następuje:

OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:**Przesłanki wykluczenia z postępowania**

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy Pzp.
2. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust 1 i art. 109 ust. 1 pkt. 4, 5, 7 ustawy Pzp .
3. Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ustawy Pzp (podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2, 5 lub art. 109 ust. 1 pkt 4, 5, 7 ustawy Pzp). Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 pkt 1 ustawy Pzp podjąłem następujące środki naprawcze i zapobiegawcze:
4. Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. poz. 835).
5. Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

*niewłaściwe skreślić

Wykonawca:

(nazwa firmy oraz adres wykonawcy)

(NIP, REGON, KRS)

(nr tel, adres e-mail)

OŚWIADCZENIE O PRZYNALEŻNOŚCI LUB BRAKU PRZYNALEŻNOŚCI DO TEJ SAMEJ GRUPY KAPITAŁOWEJ

Ja/my niżej podpisani:

.....

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

działając w imieniu i na rzecz:

.....

(pełna nazwa Wykonawcy/Wykonawców w przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia)

Ubiegając się o udzielenie zamówienia publicznego oświadczamy, że:

- 1) należymy** do tej samej grupy kapitałowej, o której mowa w art. 108 ust. 1 pkt. 5 ustawy Pzp, co podmioty wymienione poniżej*:

Lp.	Nazwa podmiotu	Adres podmiotu
1.		
2.		
....		

Jednocześnie załączam dokumenty/informacje (wymienić poniżej i załączyć do oferty):

-

-

potwierdzające, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w przedmiotowym postępowaniu.

- 2) nie należymy** do grupy kapitałowej, o której mowa w art. 108 ust. 1 pkt. 5 ustawy Pzp.

1. Uwaga! Należy wypełnić pkt. 1 lub pkt. 2.
2. Niniejszy formularz składa tylko Wykonawca wezwany przez Zamawiającego.
3. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia składa go każdy z członków konsorcjum lub wspólników spółki cywilnej.

Podmiot udostępniający zasoby:

(nazwa firmy oraz adres wykonawcy)

(NIP, REGON, KRS)

(nr tel, adres e-mail)

ZOBOWIĄZANIE DO ODDANIA DO DYSPOZYCJI WYKONAWCY NIEZBĘDNYCH ZASOBÓW NA POTRZEBY REALIZACJI ZAMÓWIENIA

Na potrzeby postępowania o udzielenie zamówienia publicznego oświadczam, co następuje:

.....

(nazwa i adres **podmiotu udostępniającego zasoby**)**Zobowiązuję się do oddania do dyspozycji:**

.....

(nazwa i adres **wykonawcy**, któremu podmiot udostępniający oddaje do dyspozycji zasoby)

niezbędnych zasobów na potrzeby realizacji zamówienia:

1. Zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby

.....

2. Sposób udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia

.....

3. Okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia

.....

4. Zakres realizacji usług, których wskazane zdolności dotyczą

.....

[Wzór oświadczenia Wykonawców wspólnie ubiegających się o udzielenie zamówienia]

Oświadczenie składane na podstawie art. 117 ust. 4 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych

PODMIOTY W IMIENIU KTÓRYCH SKŁADANE JEST OŚWIADCZENIE:

(nazwa firmy oraz adres wykonawcy)

(NIP, REGON, KRS)

(nr tel, adres e-mail)

(nazwa firmy oraz adres wykonawcy)

(NIP, REGON, KRS)

(nr tel, adres e-mail)

reprezentowane przez:

.....

.....

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Na potrzeby prowadzonego postępowania o udzielenie zamówienia publicznego,
prowadzonego przez, **działając jako pełnomocnik podmiotów, w imieniu których
składane jest oświadczenie, oświadczam, że:**

Wykonawca:

Wykona następujący zakres świadczenia wynikającego z umowy o zamówienie publiczne:

.....

Wykonawca:

Wykona następujący zakres świadczenia wynikającego z umowy o zamówienie publiczne:

.....

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą.

Wykonawca:

(nazwa firmy oraz adres wykonawcy)

(NIP, REGON, KRS)

(nr tel, adres e-mail)

OŚWIADCZENIE WYKONAWCY

Ja/my niżej podpisani:

.....

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

działając w imieniu i na rzecz:

.....

(pełna nazwa Wykonawcy/Wykonawców w przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia)

Ubiegając się o udzielenie zamówienia publicznego, oświadczam :

1. o braku wydania wobec mnie prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne;
2. o braku orzeczenia wobec mnie tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne

UMOWA NR [wzór]

zawarta w dniu 2025 roku w pomiędzy:

..... mającą swoją siedzibę w, ul.,
posiadającą NIP: oraz REGON, reprezentowaną przez:

..... -

przy kontrasygnacie

..... – Skarbnika Gminy

zwaną dalej Zamawiającym,

a

.....NIP:
reprezentowaną przez: zwaną dalej Wykonawcą,

została zawarta umowa następującej treści;

Podstawę zawarcia niniejszej Umowy, zwanej dalej „Umową” stanowi udzielenie zamówienia publicznego w trybie podstawowym bez negocjacji, stosownie do przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2024r., poz. 1320) zwaną dalej „ustawą Pzp”.

§ 1

PRZEDMIOT UMOWY

1. Zamawiający zleca, a Wykonawca przyjmuje do wykonania **realizację zadania pn. „.....”**
2. Przedmiot Umowy jest realizowany w ramach grantu pn. „Cyberbezpieczny Samorząd” współfinansowanego ze środków Unii Europejskiej: Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027
3. Realizacja przedmiotu umowy nastąpi zgodnie z niniejszą umową oraz zgodnie z warunkami określonymi w Specyfikacji Warunków Zamówienia (Załącznik nr 1 do umowy), ofertą Wykonawcy (Załącznik nr 2 do umowy), obowiązującymi przepisami i normami technicznymi.
4. Zakres rzeczowy przedmiotu umowy obejmuje w szczególności:
 - a.

§ 2

TERMIN REALIZACJI UMOWY

1. Wykonawca zrealizuje zamówienie w terminie **do dni [zgodnie z ofertą Wykonawcy]** od dnia zawarcia umowy
2. Za termin wykonania całego przedmiotu zamówienia uważa się datę podpisania protokołu odbioru

końcowego.

§ 3

WYNAGRODZENIE

1. Wynagrodzenie z tytułu wykonania przedmiotu umowy będzie stanowiła kwota **zł brutto** (słownie:), zgodnie z Załącznikiem nr 2 do Umowy (Oferta Wykonawcy)
2. Wynagrodzenie, o którym mowa w ust. 1 ma charakter ryczałtowy, co oznacza, że obejmuje wszelkie koszty związane z realizacją przedmiotu umowy i jest niezmiennie przez cały okres obowiązywania niniejszej umowy. Wynagrodzenie uwzględnia również wszelkie koszty prac niewymienionych w dokumentacji i w niniejszej umowie, a niezbędne do wykonania całości przedmiotu umowy zgodnie z umową oraz obowiązującymi przepisami prawa.
3. Wynagrodzenie z tytułu realizacji przedmiotu umowy obejmuje w szczególności wszystkie koszty związane z wykonaniem dostawy, koszty instruktażu, koszty wszystkich licencji, koszty serwisu, a także koszt udzielonej gwarancji.

§ 4

SPOSÓB PŁATNOŚCI

1. Podstawą wypłaty wynagrodzenia jest protokół odbioru prac za realizację Etapu, podpisany ze strony Zamawiającego.
2. Wynagrodzenie, o którym mowa w § 3 ust. 1 niniejszej umowy płatne będzie przelewem, na rachunek bankowy Wykonawcy wskazany w fakturze, w terminie do 30 dni od dnia otrzymania przez Zamawiającego prawidłowo wystawionej faktury.
3. Błędnie wystawiona faktura spowoduje, że 30-dniowy termin płatności, rozpocznie swój bieg od dnia dostarczenia prawidłowo wystawionej faktury, stanowiącej podstawę do uiszczenia zapłaty.
4. Wykonawca ponosi odpowiedzialność za rzetelność, prawidłowość i terminowość rozliczenia wszelkich podatków i innych należności publicznoprawnych podlegających doliczeniu do ceny.
5. Faktura wystawiona przez Wykonawcę powinna zawierać następujące określenie w polu „nabywca/odbiorca”:
GMINA WIELKA NIESZAWKA,
ul. Toruńska 12
87-165 Cierpice
NIP 879-259-36-80
6. Płatność faktury będzie dokonywana przez Zamawiającego przelewem z rachunku bankowego na rachunek Wykonawcy w banku: nr rachunku: Warunkiem zapłaty wynagrodzenia przez Zamawiającego na wskazany przez Wykonawcę rachunek jest figurowanie podanego rachunku w elektronicznym wykazie czynnych podatników VAT, prowadzonym przez Szefa Krajowej Administracji Skarbowej (tzw. biała lista podatników VAT).
7. W przypadku wskazania na fakturze rachunku bankowego nieujawnionego w wykazie podatników VAT, Zamawiający uprawniony będzie do dokonania płatności na inny rachunek bankowy ujawniony w wykazie podatników VAT lub do zapłaty na rachunek bankowy podany na fakturze z jednoczesnym powiadomieniem właściwego naczelnika urzędu skarbowego.
8. Za dzień zapłaty wynagrodzenia uważa się dzień obciążenia rachunku bankowego Zamawiającego. W przypadku konsorcjum, płatność nastąpi na konto lidera konsorcjum.

9. W razie nieterminowej zapłaty faktury Zamawiający zobowiązuje się do zapłaty ustawowych odsetek.

§ 5

OBOWIĄZKI WYKONAWCY

1. Wykonawca zobowiązuje się w szczególności do:
 - a) wykonania przedmiotu umowy określonego w § 1 z należytą starannością, na warunkach określonych w SWZ (Załącznik nr 1 do umowy), obowiązującymi przepisami i normami technicznymi i złożoną przez Wykonawcę ofertą (Załącznik nr 2 do umowy) oraz w terminie wskazanym w § 2 ust. 1 niniejszej umowy.
 - b) niezwłocznego informowania Zamawiającego na piśmie o przewidywanych opóźnieniach w realizacji przedmiotu umowy i ich przyczynach oraz o wszystkich okolicznościach po jego stronie mogących mieć wpływ na nieterminową realizację przedmiotu umowy,
 - c) współpracy z Zamawiającym, w tym udzielania wyjaśnień dotyczących sposobu realizacji przedmiotu umowy oraz informacji dotyczących postępu prac i wyników tych prac,
 - d) przestrzegania wytycznych Zamawiającego o ochronie udostępnionych informacji,
 - e) przestrzegania przepisów o ochronie danych osobowych,
 - f) zapewnienia oznakowania promocyjnego projektu współfinansowanego z Unii Europejskiej na materiałach/dokumentach dostarczanych Zamawiającemu zgodnie z obowiązującymi wytycznymi Instytucji Zarządzającej oraz wskazówkami Zamawiającego w tym zakresie.
2. Wykonawca oświadcza, że w przypadku powierzenia mu danych osobowych osób fizycznych przez Zamawiającego będzie w pełnym zakresie przestrzegać przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U.UE.L. z 2016 Nr 119 poz.1).
3. Wykonawca odpowiada prawnie i materialnie za wszelkie udostępnione mu dane/materiały, jest zobowiązany do ich zabezpieczenia przed dostępem osób nieupoważnionych, uszkodzeniem oraz nieuprawnioną zmianą ich zawartości oraz przed ich wykorzystaniem niezgodnym z celem, dla którego zostały przekazane, a także jest odpowiedzialny za ich bezpieczeństwo i integralność. Po zakończeniu realizacji zamówienia, Wykonawca zobowiązany jest do zniszczenia wszelkich kopii danych/materiałów będących w jego posiadaniu.
4. Wykonawca odpowiada za zachowanie poufności, o której mowa w niniejszym paragrafie przez wszystkie osoby, którymi posługuje się przy wykonaniu przedmiotu umowy.
5. Wykonawca zwolniony jest z obowiązku zachowania poufności jeżeli informacje, co do których taki obowiązek istniał muszą być ujawnione zgodnie z przepisami prawa lub postanowieniami sądów lub innych upoważnionych organów państwa lub muszą być ujawnione w celu wykonania przedmiotu umowy, a Wykonawca uzyskał pisemną zgodę Zamawiającego na ich ujawnienie.
6. Obowiązek zachowania poufności jest nieograniczony w czasie, jego uchylenie może być dokonane wyłącznie przez Zamawiającego w formie pisemnej pod rygorem nieważności.

§ 6

OBOWIĄZKI ZAMAWIAJĄCEGO

1. Zamawiający zobowiązuje się w szczególności do:
 - a) zapewnienia Wykonawcy dostępu do systemu informatycznego, infrastruktury Zamawiającego,
 - b) udzielania Wykonawcy informacji oraz przekazywania wszelkich danych w zakresie niezbędnym do wykonania przez Wykonawcę zobowiązań wynikających z niniejszej umowy, w tym dostępu do posiadanych przez Zamawiającego i niezbędnych do realizacji niniejszej umowy dokumentów, opracowań i materiałów,

- c) zapewnienia dostępności pracowników merytorycznych na poszczególnych stanowiskach pracy,
 - d) zapłaty wynagrodzenia Wykonawcy na zasadach określonych w niniejszej umowie.
2. Zamawiający zobowiązuje się do zapewnienia pracownikom Wykonawcy realizującym przedmiot umowy możliwości pracy w siedzibie Zamawiającego po uprzednim uzgodnieniu zakresu, terminów i godzin, a także zapewnienia obecności w tym czasie upoważnionego pracownika Zamawiającego.

§ 7

OSOBY REALIZUJĄCE UMOWĘ

1. Wykonawca zapewnia, że wszystkie osoby wyznaczone przez niego do realizacji umowy posiadają odpowiednie kwalifikacje oraz przeszkolenia i uprawnienia, jeśli są wymagane przepisami prawa.
2. W imieniu Wykonawcy osobą upoważnioną do kontaktów z Zamawiającym w przedmiocie umowy jest Pan/Pani tel. e-mail:
3. We wszystkich sprawach związanych z wykonaniem umowy Wykonawca kontaktować się będzie bezpośrednio i wyłącznie z Zamawiającym, w imieniu którego występował/-a będzie Pan/Pani tel. e-mail:
4. Za nadzór nad realizacją umowy ze strony Zamawiającego odpowiedzialni są:
 - a) – e-mail:, tel.,
 - b) – e-mail:, tel.
 Strony zobowiązują się do niezwłocznego przekazywania wszelkich informacji, mogących mieć znaczenie dla realizacji przedmiotu umowy.
5. Dokonywanie ustaleń istotnych z punktu widzenia realizacji niniejszej umowy, wymaga udokumentowanej formy (co najmniej e-mail na adres podany w niniejszym paragrafie; w przypadku oświadczeń woli składanych przez strony wymagana jest forma pisemna).

§ 8

ZASADY ODBIORU

1. Wykonawca zgłasza w formie pisemnej Zamawiającemu gotowość do odbioru przedmiotu umowy, o którym mowa w § 1 niniejszej umowy. Najpóźniej na następny dzień roboczy po zgłoszeniu przez Wykonawcę gotowości do odbioru spisany zostanie protokół zdawczo – odbiorczy, jednakże nie stanowi on potwierdzenia prawidłowego wykonania prac. Stanowi on jedynie potwierdzenie terminu, w którym Wykonawca przekazał przedmiot umowy do odbioru. Przyjęcie przedmiotu umowy do sprawdzenia nie jest równoznaczne z odbiorem prac i nie upoważnia Wykonawcy do wystawienia faktury.
2. Zamawiający w terminie do 7 dni kalendarzowych od dnia spisania protokołu zdawczo - odbiorczego dokona sprawdzenia zgłoszonego do odbioru przedmiotu umowy.
3. Jeżeli sprawdzenie zakończy się wynikiem pozytywnym, spisany zostanie protokół odbioru końcowego.
4. W przypadku braku możliwości dokonania sprawdzenia lub wykrycia w trakcie sprawdzania wad uniemożliwiających użytkowanie oprogramowania zgodnie z jego przeznaczeniem lub braku możliwości osiągnięcia funkcjonalności oprogramowania, Zamawiający wezwie Wykonawcę (mailem) do usunięcia usterek.
5. Wykonawca usunie usterki, o których mowa w ust. 4 na własny koszt w terminie do 7 dni kalendarzowych od dnia wezwania.
6. W przypadku, gdyby czynności wykonawcy nie doprowadziły do usunięcia usterek, o których mowa wyżej, Zamawiający może wyznaczyć Wykonawcy dodatkowy czas na ich usunięcie nie dłuższy jednak niż 5 dni kalendarzowych.
7. Brak usunięcia usterek w dodatkowym terminie, o którym mowa w ust. 6, skutkować będzie naliczeniem kar

umownych określonych w § 10 ust. 2 pkt 2).

8. Za datę wykonania przedmiotu umowy uznaje się dzień podpisania przez Zamawiającego protokołu odbioru końcowego.

§ 9

PRZETWARZANIE DANYCH OSOBOWYCH

1. Na mocy niniejszej umowy jako Administrator danych osobowych Zamawiającego, na podstawie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zwanego w dalszej części „RODO” powierza Wykonawcy, dane osobowe do przetwarzania, na zasadach określonych w niniejszej umowie oraz w celu i zakresie niezbędnym do realizacji przedmiotu niniejszej umowy.
2. Czas trwania przetwarzania powierzonych Wykonawcy danych osobowych będzie zgodny z okresem realizacji przedmiotu niniejszej umowy.
3. Przetwarzanie powierzonych danych osobowych przez Wykonawcę będzie obejmowało czynności na danych osobowych niezbędne do realizacji przedmiotu umowy.
4. Wykonawca zapewnia, że:
 - a) posiada fachową wiedzę i zasoby konieczne do należytej realizacji niniejszej umowy, w szczególności wdrożył środki techniczne i organizacyjne, w tym te dotyczące wymogów bezpieczeństwa przetwarzania, odpowiadające wymogom określonym w RODO,
 - b) będzie zabezpieczał interes prawny osób, których dane przetwarza;
 - c) będzie realizował wytyczne Administratora Zamawiającego w zakresie bezpieczeństwa przetwarzanych powierzonych mu danych, w zakresie wprost wynikającym z przepisów prawa powszechnego oraz wewnętrznych regulacji Zamawiającego,
 - d) dane osobowe będą przetwarzane na terenie Unii Europejskiej i nie będą przekazane do państwa trzeciego lub organizacji międzynarodowej spoza Unii Europejskiej.
5. Wykonawca zobowiązany jest do przetwarzania danych osobowych wyłącznie w celach związanych z wykonywaniem niniejszej umowy oraz uprawniony jest do przetwarzania danych osobowych wyłącznie w takim zakresie, w jakim zostało mu to powierzone przez Zamawiającego.
6. Wykonawca zobowiązany jest wykonywać wszelkie czynności związane z przetwarzaniem powierzonych danych osobowych z zachowaniem szczególnej staranności.
7. Zamawiający ponosi pełną odpowiedzialność za fizyczne bezpieczeństwo danych zgromadzonych w wersji papierowej i cyfrowej w lokalnych bazach danych, a w szczególności za ich kradzież lub wyniesienie z siedziby Zamawiającego.
8. Zamawiający wyraża zgodę Wykonawcy na dalsze powierzenie podwykonawcom przetwarzania danych osobowych w celu i zakresie niezbędnym do realizacji niniejszej umowy. Podpowierzenie nie może nastąpić w innym celu i zakresie niż powierzenie przetwarzania danych osobowych na podstawie niniejszej umowy. Wykonawca w pisemnych umowach z podwykonawcami, zapewni odpowiednie stosowanie zasad i warunków przetwarzania danych osobowych, zgodnie z wymogami obowiązujących przepisów prawa o ochronie danych osobowych.
9. Jeżeli Wykonawca korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają na mocy umowy te same obowiązki ochrony danych jak w umowie z Zamawiającym. W szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych. Jeżeli inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Zamawiającego za wypełnienie obowiązków innego podmiotu przetwarzającego spoczywa na Wykonawcy.

10. W sytuacjach nadzwyczajnych, nie przewidzianych w niniejszej umowie, Wykonawca zobowiązuje się do przetwarzania danych osobowych mając na uwadze ochronę danych oraz interes Zamawiającego.
11. Wykonawca uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych różnym prawdopodobieństwie wystąpienia i wadze zagrożenia zapewnia wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, tak by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
12. Wykonawca zapewnia, aby każda osoba przetwarzająca w jej imieniu dane osobowe miała imienne upoważnienie do przetwarzania danych osobowych.
13. Wykonawca zobowiązuje się do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.
14. Wykonawca zapewnia, że osoby upoważnione do przetwarzania danych osobowych zobowiążą się do zachowania tajemnicy danych osobowych w trakcie trwania umowy oraz po jej zakończeniu. Wykonawca zobowiązuje się na każde żądanie Zleceniodawcy okazać stosowne dokumenty poświadczające zobowiązanie do poufności.
15. Wykonawca ponosi odpowiedzialność za działania i zaniechania osób przez niego upoważnionych do przetwarzania danych osobowych.
16. Wykonawca udostępnia Zamawiającemu wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w przepisach prawa dotyczących ochrony danych osobowych, oraz umożliwia Zamawiającemu przeprowadzanie audytów.
17. Wykonawca zobowiązuje się do zachowania w tajemnicy danych osobowych powierzonych mu w związku z wykonywaniem umowy, a w szczególności do tego, że nie będzie w okresie obowiązywania umowy i po jej rozwiązaniu: przekazywać, wykorzystywać lub ujawniać danych osobowych uzyskanych od Zamawiającego osobom nieupoważnionym.
18. Strony umowy zobowiązują się ściśle współpracować podczas realizacji umowy w zakresie dotyczącym przetwarzania danych osobowych na podstawie niniejszej umowy, w szczególności obowiązek współpracy dotyczy wzajemnego przekazywania informacji oraz dokonywania ustaleń w zakresie bezpieczeństwa danych osobowych przez osoby pełniące funkcje Inspektorów Ochrony Danych u Zamawiającego i Wykonawcy.
19. Wykonawca zobowiązany jest do raportowania Zamawiającemu wszelkich incydentów związanych z bezpieczeństwem powierzonych do przetwarzania danych osobowych. Wykonawca jest zobowiązany niezwłocznie zgłosić Zamawiającemu każde stwierdzone naruszenie ochrony danych osobowych.
20. Wykonawca zobowiązany jest do umożliwienia przeprowadzenia przez właściwy organ administracji kontroli zgodności przetwarzania danych osobowych z przepisami prawa.
21. Wykonawca zobowiązany jest do niezwłocznego poinformowania Zamawiającego o podjęciu przez uprawniony organ jakichkolwiek działań względem Wykonawcy w zakresie kontroli przetwarzania danych osobowych przez Wykonawcę, w szczególności informacji o zapowiedzi kontroli oraz rozpoczęciu takiej kontroli przez uprawniony organ, jeśli kontrola dotyczy sposobu przetwarzania powierzonych przez Zamawiającego danych osobowych.
22. Wykonawca zobowiązany jest do przekazania Zamawiającemu wszelkich informacji dotyczących zakresu, wyników oraz działań podjętych przez uprawniony organ w wyniku przeprowadzonej kontroli, jeśli kontrola dotyczy przetwarzania powierzonych przez Zamawiającego danych osobowych.
23. Za przetwarzanie danych osobowych niezgodnie z przepisami prawa ochrony danych osobowych lub postanowieniami niniejszej umowy i za jakiegokolwiek naruszenia zakresu i celu ich przetwarzania, Wykonawca ponosi wobec Zamawiającego pełną odpowiedzialność.
24. Z chwilą rozwiązania umowy Wykonawca stosownie do decyzji Zamawiającego zobowiązuje się zaprzestać przetwarzania danych osobowych, usunąć lub zwrócić powierzone do przetwarzania dane osobowe w tym istniejące kopie, z uwzględnieniem obowiązujących przepisów prawa dot. obowiązku przechowywania danych.

25. Strony umowy postanawiają, że w zakresie dotyczącym przetwarzania danych osobowych na podstawie niniejszej umowy, w szczególności współpracy i wzajemnego przekazywania informacji oraz dokonywania ustaleń w zakresie bezpieczeństwa danych osobowych będą się kontaktowały za pośrednictwem następujących osób:

- · ze strony Administratora Zamawiającego:
- · ze strony Wykonawcy:

§ 10

KARY UMOWNE

1. Wykonawca zobowiązany jest zapłacić Zamawiającemu karę umowną w wysokości 20% maksymalnego wynagrodzenia umownego brutto, określonego w § 3 ust. 1, w przypadku odstąpienia przez Wykonawcę lub Zamawiającego od umowy z powodu okoliczności, za które odpowiada Wykonawca.
2. Wykonawca zobowiązany jest do zapłaty na rzecz Zamawiającego kar umownych w następujących przypadkach i we wskazanej niżej wysokości:
 - 1) 0,5% wynagrodzenia umownego brutto, określonego w § 3 ust. 1 umowy, za każdy dzień zwłoki w przekazaniu Zamawiającemu przedmiotu umowy w terminie określonym odpowiednio w § 2 ust. 1 umowy;
 - 2) 0,05% wynagrodzenia umownego brutto, określonego w § 3 ust. 1 umowy, za każdy dzień zwłoki w usunięciu usterek w dodatkowym terminie;
 - 3) 0,25% wynagrodzenia umownego brutto, określonego w § 3 ust. 1 umowy, za każdy dzień zwłoki w realizacji zobowiązań wynikających z § 13 ust. 4 umowy;
 - 4) 0,25% wynagrodzenia umownego brutto, określonego w § 3 ust. 1 umowy, za każdą godzinę zwłoki w realizacji zobowiązań wynikających z § 13 ust. 5 umowy;
3. Jeżeli zwłoka, o której mowa w ust. 2 pkt 1 przekroczy 14 dni, Zamawiający zastrzega sobie prawo odstąpienia od Umowy w całości lub części z powodu okoliczności, za które odpowiada Wykonawca, w terminie do 30 dni od dnia stwierdzenia przez Zamawiającego przestanki uprawniającej do odstąpienia od Umowy, z jednoczesnym prawem do kary umownej w wysokości określonej w ust. 1.
4. Jeżeli na skutek niewykonania lub nienależytego wykonania Umowy powstanie szkoda przewyższająca zastrzeżone kary umowne, Zamawiającemu oprócz tych kar przysługuje prawo do dochodzenia odszkodowania uzupełniającego. Jeżeli szkoda powstanie z innych przyczyn niż te, ze względu na które zastrzeżono karę umowną, Zamawiającemu przysługuje prawo do dochodzenia odszkodowania na zasadach ogólnych Kodeksu cywilnego.
5. Kary umowne, o których mowa w ust. 2, są naliczane niezależnie i podlegają sumowaniu. Suma kar umownych nałożonych na Wykonawcę nie może przekroczyć 20 % wynagrodzenia umownego brutto.
6. Dla uniknięcia wątpliwości Strony zgodnie oświadczają, że przy dochodzeniu kar umownych Zamawiający nie ma obowiązku wykazywania poniesionej szkody.
7. Wykonawca wyraża zgodę na potrącenia kar umownych z wynagrodzenia, o którym mowa w § 3 ust. 1 umowy, co będzie dokumentowane odpowiednią notą księgową wystawioną przez Zamawiającego.

§ 11

ODSTĄPIENIE OD UMOWY

1. Poza przypadkami wskazanymi w niniejszej umowie, Zamawiającemu przysługuje prawo odstąpienia od umowy w całości lub części w przypadkach, gdy:
 - 1) wystąpi istotna zmiana okoliczności powodująca, że wykonanie umowy nie leży w interesie publicznym,

czego nie można było przewidzieć w chwili zawarcia umowy, lub dalsze wykonywanie umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu; w takim przypadku Wykonawca może odstąpić od umowy w terminie 30 dni od dnia powzięcia wiadomości o tych okolicznościach;

- 2) przedmiot umowy realizowany jest w sposób sprzeczny z przepisami prawa lub uprzednio wskazanymi przez Zamawiającego wytycznymi (zarządzeniami, decyzjami itp.);
 - 3) Wykonawca istotnie narusza warunki umowy i nie zaprzestanie lub nie naprawi skutków naruszenia po upływie 14 dni od dnia wezwania przez Zamawiającego;
 - 4) Wykonawca nie rozpoczął prac lub przerwał prace na okres dłuższy niż 14 dni oraz nie kontynuuje ich pomimo wezwania Zamawiającego;
 - 5) Wykonawca opóźnia się z realizacją przedmiotu umowy tak dalece, że nie jest prawdopodobnym ukończenie realizacji umowy w wyznaczonym terminie;
 - 6) bezskutecznie upłyne termin wyznaczony na poprawienie przez Wykonawcę przedmiotu umowy zawierającego braki i błędy;
 - 7) po poprawieniu przedmiot umowy nadal wykonany jest w sposób sprzeczny z umową i zawiera braki i błędy;
 - 8) utraty środków pochodzących z budżetu Projektu, na realizację umowy;
 - 9) zostanie ogłoszona upadłość lub przeprowadzona likwidacja Wykonawcy;
 - 10) w trybie postępowania egzekucyjnego zostanie zajęty majątek Wykonawcy i Wykonawca nie będzie mógł realizować umowy na warunkach w niej określonych;
 - 11) nastąpi ograniczenie lub pozbawienie zdolności do czynności prawnych mających wpływ na realizację umowy;
 - 12) Trybunał Sprawiedliwości Unii Europejskiej stwierdzi, w ramach procedury przewidzianej w art. 258 Traktatu o Funkcjonowaniu Unii Europejskiej, że państwo polskie uchybiło zobowiązaniom, które ciąży na nim na mocy Traktatów, dyrektywy 2014/24/UE i dyrektywy 2014/25/UE, z uwagi na to, że zamawiający udzielił zamówienia z naruszeniem przepisów prawa Unii Europejskiej;
 - 13) Wykonawca w chwili zawarcia umowy podlegał wykluczeniu z postępowania na podstawie art. 108 ustawy Pzp.
2. W przypadku otwarcia likwidacji, złożenia wniosku o upadłość lub wydania sądowego nakazu zajęcia majątku Wykonawcy, Zamawiający ma prawo odstąpić od umowy z zachowaniem 30 dniowego okresu wypowiedzenia.
 3. Odstąpienie od umowy w sytuacjach określonych w ust. 1 może nastąpić w terminie 30 dni od daty powzięcia informacji przez Zamawiającego o powyższych okolicznościach.
 4. Odstąpienie od umowy następuje w formie pisemnej pod rygorem nieważności ze wskazaniem podstawy odstąpienia.
 5. W wypadku odstąpienia od Umowy którejkolwiek ze Stron, w terminie 7 dni od daty odstąpienia Wykonawca, przy udziale Zamawiającego, sporządzi szczegółowy protokół inwentaryzacji wykonanych prac według stanu na dzień odstąpienia.
 6. Koszty dodatkowe poniesione na zabezpieczenie prac oraz wszelkie inne uzasadnione koszty związane z odstąpieniem od umowy ponosi Strona, z której winy doszło do odstąpienia od umowy.

§ 12

ZMIANY UMOWY

1. Strony dopuszczają możliwość zmiany postanowień Umowy w stosunku do treści oferty, na podstawie, której dokonano wyboru wykonawcy w następujących przypadkach w następujących okolicznościach i warunkach:
 - a) zmiany terminu realizacji przedmiotu umowy, w następstwie:

- siły wyższej - rozumianej jako wystąpienie zdarzenia nadzwyczajnego, zewnętrznego, niemożliwego do przewidzenia i zapobieżenia, którego nie dało się uniknąć nawet przy zachowaniu najwyższej staranności, a które uniemożliwia Wykonawcy wykonanie przedmiotu umowy. W razie wystąpienia siły wyższej strony umowy zobowiązane są dołożyć wszelkich starań w celu ograniczenia do minimum opóźnień w wykonywaniu swoich zobowiązań umownych, powstałego na skutek działania siły wyższej,
 - okoliczności leżących po stronie Zamawiającego i nie wynikających z przyczyn leżących po stronie Wykonawcy (np. wstrzymanie, zawieszenie, przerwa w realizacji),
 - przestojów i opóźnień zawinionych przez Zamawiającego,
 - wystąpienia okoliczności, których strony umowy nie były w stanie przewidzieć, pomimo zachowania należytej staranności,
 - przyczyn niezależnych od którejkolwiek ze stron, które w szczególności dotyczyć będą uwarunkowań formalno-prawnych. Termin wykonania umowy ulega odpowiednio zmianie o okres trwania okoliczności celem ukończenia przedmiotu umowy w sposób należyty. Zmiana terminu realizacji przedmiotu umowy nie wpływa na zmianę wynagrodzenia.
- b) zmiana - ograniczenie (rezygnacja) z części zakresu przedmiotu umowy przez Zamawiającego z uzasadnionych przyczyn, mających charakter obiektywny, co spowoduje odpowiednie zmniejszenie wynagrodzenia Wykonawcy;
- c) zmiany wynagrodzenia Wykonawcy:
- w następstwie zmiany będącej skutkiem działań organów państwowych, przez co należy rozumieć ustawową zmianę obowiązującej stawki podatku,
 - w wyniku ograniczenia (rezygnacji) z części zakresu przedmiotu umowy, co spowoduje odpowiednie zmniejszenie wynagrodzenia Wykonawcy;
- d) zmiany powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację przedmiotu zamówienia lub świadczenia stron,
- e) zmiany, rezygnacji bądź wprowadzenia podwykonawcy w trakcie realizacji umowy w zakresie nie przewidzianym w ofercie,
- f) powstania rozbieżności lub niejasności w rozumieniu pojęć użytych w umowie, których nie będzie można usunąć w inny sposób, a zmiana będzie umożliwiać usunięcie rozbieżności i doprecyzowanie umowy w celu jednoznacznej interpretacji jej zapisów przez strony.
2. Wszystkie powyższe postanowienia stanowią katalog zmian, na które Zamawiający może wyrazić zgodę. Nie stanowią jednocześnie zobowiązania do wyrażenia takiej zgody.
3. W sytuacji wystąpienia okoliczności, o których wyżej mowa, każda ze stron może wystąpić z wnioskiem zawierającym:
- a) opis propozycji zmiany, w tym wpływ na terminy wykonania,
 - b) uzasadnienie zmiany.
4. Zmianie podlegają także wszelkie nieistotne postanowienia umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy, w tym m.in.:
- a) zmiana osób wyznaczonych do realizacji umowy, ze strony Zamawiającego w przypadku braku możliwości nadzoru przez te osoby - zmiana ta nie wymaga zawarcia aneksu do umowy,
 - b) zmiana danych związana z obsługą administracyjno-organizacyjną umowy (danych teleadresowych Wykonawcy; Zamawiającego, zmiana rachunku bankowego) - zmiana ta następuje poprzez pisemne zgłoszenie tego faktu drugiej stronie i nie wymaga zawarcia aneksu do umowy,
 - c) przekształcenie Wykonawcy w związku z sukcesją generalną, przekształceniami, dziedziczeniem spółek handlowych zgodnie z KSH, a także sukcesją z mocy prawa, zgodnie z obowiązującymi przepisami (następstwa prawne) winno nastąpić w formie aneksu do umowy.
5. Wszelkie zmiany i uzupełnienia niniejszej umowy dokonane w sposób zgodny z ustawą Prawo zamówień

publicznych wymagają formy pisemnej pod rygorem nieważności - aneks do umowy, z zastrzeżeniem przypadków określonych w niniejszym paragrafie, w których wskazano, że nie jest wymagane zawarcie aneksu do umowy.

6. Zmiana umowy dokonana z naruszeniem przepisów ustawy Prawo zamówień publicznych podlega unieważnieniu.
7. Strony zgodnie ustalają, że Wykonawca nie może dokonać cesji jakichkolwiek praw lub obowiązków wynikających z tej umowy, bez pisemnej zgody Zamawiającego.

§ 13 RĘKOJMIA, GWARANCJA

1. Wykonawca gwarantuje Zamawiającemu, że wykonany i dostarczony do Zamawiającego przedmiot umowy będzie należytej jakości, wolny od wad oraz będzie spełniać wszelkie wymagania określone w SWZ, Opisie przedmiotu zamówienia oraz niniejszej umowie.
2. Wykonawca udziela gwarancji na dostarczane w ramach umowy sprzęt i oprogramowanie na okres wskazany w SWZ
3. Wykonawca zapewni w okresie gwarancji usługę serwisu na warunkach wskazanych w SWZ
4. Okres gwarancji wskazany w ust. 2 liczy się od daty podpisania przez obie strony protokołu odbioru końcowego przedmiotu umowy.
5. Okres gwarancji ulega wydłużeniu o czas liczony od zawiadomienia Wykonawcy o wystąpieniu wady/usterki do momentu jej usunięcia.
6. Odpowiedzialność z tytułu gwarancji obejmuje zarówno wady/usterki powstałe z przyczyn tkwiących w przedmiocie umowy w chwili dokonania jego odbioru przez Zamawiającego.
7. Gwarancja obejmuje w szczególności:
 - a) poprawne działanie dostarczonego i wdrożonego rozwiązania w zakresie realizacji funkcji zgodnych z OPZ,
 - b) poprawność wdrożonego rozwiązania w zakresie braku wad fizycznych i prawnych,
 - c) poprawność uruchomionych i wdrożonych aplikacji, sprzętu, usług i procedur,
 - d) zapewnienie prawidłowego działania przedmiotu umowy w okresie gwarancji,
8. Wykonawca zapewnia w czasie realizacji umowy oraz w trakcie prac serwisowych komunikację pracowników Zamawiającego z przedstawicielami Wykonawcy oraz firmą/osobami wykonującymi prace serwisowe w języku polskim.
9. Wszelkie świadczenia Wykonawcy w okresie gwarancji są bezpłatne i nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów.
10. Okres rękojmi jest równy okresowi gwarancji.
11. Wykonawca odpowiada za wady fizyczne i prawne ujawnione w dostarczonym oprogramowaniu oraz ponosi z tego tytułu wszelkie zobowiązania opisane w niniejszej umowie oraz wynikające z obowiązującego prawa. Wykonawca jest odpowiedzialny względem Zamawiającego, jeżeli dostarczony przedmiot umowy w szczególności:
 - a) stanowi własność osoby trzeciej, albo jeżeli jest obciążony prawem osoby trzeciej,
 - b) ma wady zmniejszające jego wartość lub użyteczność ze względu na cel określony w załączonym Opisie przedmiotu zamówienia, albo wynikający z okoliczności lub z przeznaczenia rzeczy,
 - c) nie ma właściwości wymaganych przez Zamawiającego,
 - d) jest w stanie niekompletnym.
12. O wadzie fizycznej lub prawnej przedmiotu umowy Zamawiający zawiadamia Wykonawcę bezpośrednio, w celu realizacji przysługujących z tego tytułu uprawnień. Formę zawiadomienia stanowi „Protokół reklamacji” sporządzony przez Zamawiającego lub jego przedstawiciela oraz przekazany Wykonawcy.
13. Wykonawca jest zobowiązany do usunięcia wad fizycznych i prawnych przedmiotu umowy lub do dostarczenia przedmiotu umowy wolnego od wad, jeżeli wady te ujawnią się w okresie gwarancji.

§ 14

WARUNKI LICENCJI

1. Wykonawca udziela Zamawiającemu licencji na warunkach określonych w umowie.
2. Wykonawca nie będzie uprawniony do wypowiedzenia Licencji, o ile zamawiający nie naruszy jej postanowień.
3. Na podstawie udzielonej Licencji, Zamawiający uprawniony będzie do użytkowania oprogramowania w zakresie wynikającym z jego charakteru i przeznaczenia, wyłącznie na użytek realizacji zadań własnych bez prawa dystrybucji, użyczania, wynajmowania, wdzierżawiania, udzielania dalszych sublicencji lub innego przenoszenia swych praw na osoby trzecie.
4. Licencje nie mogą narzucać konieczności używania oprogramowania łącznie z innym oprogramowaniem, którego pozyskanie będzie obowiązkiem Zamawiającego, nie wynikającym z postanowień umowy i Opisu przedmiotu zamówienia stanowiącego załącznik do umowy, ani ponoszenia przez Zamawiającego dodatkowych opłat.
5. Licencje uprawniają do korzystania z utworów co najmniej na terytorium Rzeczypospolitej Polskiej.
6. Licencje nie są ograniczone co do liczby użytkowników lub charakterystyk związanych z technologią środowiska informatycznego, w którym będzie używane oprogramowanie i dotyczą wszystkich struktur organizacyjnych Zamawiającego, istniejących lub powstałych w przyszłości, a także będących jego następcami prawnymi, chyba, że szczegółowe postanowienia zawarte w Opisie przedmiotu zamówienia stanowią inaczej w odniesieniu do określonych elementów zamówienia.
7. Udzielenie Licencji na warunkach określonych w niniejszym paragrafie zostanie potwierdzone stosownym dokumentem licencyjnym (certyfikatem), podpisanym przez osobę(y) uprawnioną do jej udzielenia.
8. Wykonawca oświadcza, że w przypadku, gdy do realizacji niniejszej umowy wykorzysta oprogramowanie tzw. open source:
 - a) nie ograniczy to żadnych uprawnień Zamawiającego z niniejszej umowy ani obowiązków Wykonawcy z tytułu serwisu ani gwarancji,
 - b) Wykonawca dostarczy Zamawiającemu treści licencji tego oprogramowania na zasadach, na których jest ono rozpowszechniane

§ 15

PODWYKONAWCY

1. Wykonawca może korzystać przy realizacji przedmiotu umowy z podwykonawców na zasadach określonych w art. 462 ustawy Prawo Zamówień Publicznych oraz opisanych w niniejszym paragrafie i za zgodą Zamawiającego.
2. Wykonawca zamierzający zawrzeć umowę o podwykonawstwo, której przedmiotem są dostawy, jest obowiązany, w trakcie realizacji niniejszej umowy i przed zawarciem umowy z podwykonawcą, do przedłożenia Zamawiającemu projektu tej umowy.
3. W trakcie realizacji umowy Wykonawca może dokonać zmiany podwykonawcy, zrezygnować z podwykonawcy bądź wprowadzić podwykonawcę w zakresie nieprzewidzianym w ofercie.
4. Jeżeli zmiana lub rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się, na zasadach określonych w art. 118 ustawy Prawo Zamówień Publicznych, w celu wykazania spełnienia warunków udziału w postępowaniu, Wykonawca jest obowiązany wykazać Zamawiającemu, iż proponowany inny podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż wymagany w trakcie postępowania o udzielenie zamówienia.
5. Wykonanie części/zakresu przedmiotu umowy w podwykonawstwie nie zwalnia Wykonawcy od odpowiedzialności i zobowiązań wynikających z warunków umowy. Wykonawca będzie odpowiedzialny za

działania, uchybienia i zaniedbania podwykonawcy jak za własne działanie lub zaniechanie.

§ 16

POSTANOWIENIA KOŃCOWE

1. Wykonawca nie może, bez pisemnej zgody Zamawiającego, przenieść obowiązków wynikających z niniejszej umowy na osoby trzecie.
2. W sprawach nieuregulowanych niniejszą umową mają zastosowanie obowiązujące przepisy prawa, a w szczególności ustawy Pzp oraz Kodeksu cywilnego.
3. Wykonawca i Zamawiający poddają spory pod rozstrzygnięcie sądu właściwego dla siedziby Zamawiającego.
4. Umowę sporządzono w czterech jednobrzmiących egzemplarzach, z których trzy egzemplarze otrzymuje Zamawiający, a jeden egzemplarz otrzymuje Wykonawca.

Załączniki do umowy:

Załącznik nr 1 – Specyfikacja warunków Zamówienia,

Załącznik nr 2 – Oferta Wykonawcy.

ZAMAWIAJĄCY:

WYKONAWCA:

Wymagania dotyczące próbki przedmiotu zamówienia oraz zasady i zakres jej badania
[dotyczy CZĘŚCI III]

Wymagania ogólne

1. Zamawiający wymaga, aby Wykonawca, wraz z ofertą, złożył próbkę oferowanego oprogramowania.
2. Celem złożenia próbki jest potwierdzenie, poprzez jej badanie i wyjaśnianie, zwane dalej badaniem próbki, że oferowane przez Wykonawcę dostawy i usługi spełniają wymagania określone przez Zamawiającego w opisie przedmiotu zamówienia;
3. Próbka musi być złożona z:
 - a. nośnika danych – np. laptop, dysk zewnętrzny, pendrive
 - b. oprogramowania posiadającego funkcjonalność wskazaną w poniższym scenariuszu badania próbki wraz z danymi demonstracyjnymi
 - c. filmu prezentacyjnego z lektorem w języku polskim omawiającego oferowane oprogramowanie i poszczególne kroki scenariusza
4. Przykładowe dane demonstracyjne nie mogą naruszać zapisów Ustawy o ochronie danych osobowych. W przypadku jej naruszenia całkowitą odpowiedzialność ponosi Wykonawca.
5. Badanie próbki w zakresie oprogramowania odbędzie się w oparciu o scenariusz badania próbki opisany w Rozdziale III niniejszego załącznika.
6. Oceny czy oferowane oprogramowanie odpowiada wymaganiom określonym przez Zamawiającego dokona Komisja Przetargowa na podstawie zawartości złożonej próbki.
7. Dostarczenie sprawnych nośników danych jest obowiązkiem Wykonawcy, a ich parametry muszą pozwalać na sprawne funkcjonowanie wirtualnej maszyny z zainstalowanym systemem operacyjnym, oferowanym oprogramowaniem systemu i przykładowymi danymi, jeśli to konieczne do uruchomienia.
8. Próbka musi zawierać to samo oprogramowanie, w tej samej technologii, co system oferowany w niniejszym postępowaniu, który stanowił będzie przedmiot dostawy i wdrożenia. Zamawiający nie dopuszcza prezentacji poglądowych z użyciem oprogramowania prezentacyjnego np. Microsoft Power Point.
9. Próbka musi zostać w pełni skonfigurowana i zawierać wszystkie niezbędne elementy (sprzętowe i programowe) zapewniające możliwość praktycznej weryfikacji wymaganych funkcjonalności oprogramowania. Przekazana próbka musi być zabezpieczona hasłem/hasłami dostępu. Informacja o wszystkich danych umożliwiających uruchomienie wersji demonstracyjnej systemu, tj. nazwy użytkowników i ich hasła, muszą zostać wydrukowane i zostać umieszczone w zabezpieczonej kopercie i dołączone do zestawu demonstracyjnego. Zamawiający dopuszcza możliwość rekonfiguracji dostępu do sieci Internet (w tym przekierowania portów) celem zapewnienia poprawnej komunikacji w celu weryfikacji próbki.
10. Próbka pod względem formalnym, stanowić będzie załącznik do oferty. Powinna być zabezpieczona w odpowiednim, trwałym opakowaniu uniemożliwiającym jego zdjęcie bez rozerwania (gruba koperta, pudełko kartonowe) odpowiednio opisanym i podpisanym. Zamawiający nie przewiduje pokrycia kosztów przygotowania próbki. Zamawiający nie przewiduje wykorzystania próbki, do celów innych niż przeprowadzenia weryfikacji oprogramowania systemu.

Opis procedury badania próbki

1. Badanie próbek będzie dokonane przez Komisję Przetargową Zamawiającego.
2. Przedmiotem weryfikacji i oceny przez Komisję Przetargową Zamawiającego jest potwierdzenie, że w momencie złożenia oferty przez wykonawcę, zaoferowane oprogramowanie posiada funkcjonalności wymagane przez Zamawiającego. Weryfikacja obejmie wybrane funkcjonalności spośród wszystkich wymagań opisanych przez Zamawiającego w scenariuszu.
3. W przypadku, gdy Zamawiający weryfikując próbkę uzna, że oprogramowanie nie posiada cech/funkcjonalności oprogramowania, określonych w opisie przedmiotu zamówienia, nastąpi zakończenie procesu badania próbki i odrzucenie oferty na podstawie art. 226 ust.1 pkt 5 ustawy Pzp jako niezgodnej z warunkami zamówienia.
4. Z przeprowadzonego badania próbki Zamawiający sporządzi protokół. Przedmiotowy protokół będzie zawierał wskazanie, jakie oprogramowanie zostało zaprezentowane dla danej funkcjonalności (nazwa oprogramowania i wskazanie autora / producenta) oraz wynik badania dla każdego weryfikowanego punktu.
5. Wykonawca zobowiązany jest do udzielenia Zamawiającemu wszelkich wyjaśnień umożliwiających zbadanie, czy oferowane oprogramowanie posiada wymagane cechy i funkcjonalności.

Scenariusz badania próbki Oprogramowania umożliwiającego monitoring usług i użytkowanych systemów

Krok	Czynności do wykonania
I	Zarządzanie monitorowanymi parametrami
1	Zalogować się do systemu jako administrator.
2	Dodać obiekt1 z agentem aktywnym (push), czyli takim, gdzie agent na systemie gościa wysyła dane do systemu monitorującego. Zweryfikować poprawność dodania pozycji z aktywnym agentem.
3	Dodać obiekt2 z agentem pasywnym (pull), czyli takim, gdzie system monitorujący pobiera dane od agenta monitorowanego. Zweryfikować poprawność dodania pozycji z pasywnym agentem.
4	Przedstawić zbieranie danych z obiektów: a. zaprezentować dane z Obiektu1 za pomocą agenta w metodzie push monitorującego co najmniej dwa parametry, w tym powiadomienie o dostępie do systemu z wykorzystaniem SSH. b. zaprezentować dane z Obiektu2 za pomocą agenta w metodzie pull: monitorującego ilość wolnego miejsca na dysku i co najmniej użycie CPU
5	Zaprezentować dane zbierane w czasie rzeczywistym, zaprezentować zmianę statusu w przypadku błędu komunikacji przy próbie wysłania za pomocą modułu integracyjnego z platformą krajową, np. ePUAP, e-doręczenia (integracja ze środowiskiem testowym): a. sprawdzić status usługi w systemie monitorującym (usługa w systemie obsługującym komunikację jest wyłączona) b. zalogować się w systemie obsługującym komunikację z systemem krajowym (np. e-PUAP, e-doręczenia) i zmienić status usługi na włączona, przeprowadzić konfigurację parametrów usługi c. sprawdzić status usługi w systemie monitorującym (powinna nastąpić zmiana statusu informująca o prawidłowym działaniu) d. zalogować się w systemie obsługującym komunikację z systemem krajowym i przeprowadzić testową wysyłkę e. sprawdzić w systemie monitorującym brak komunikatów o błędach f. przeprowadzić celowy sabotaż komunikacji z platformą krajową i systemem obsługującym komunikację z systemem krajowym g. zalogować się w systemie obsługującym komunikację z systemem i wysłać testową wiadomość

- h. zweryfikować powstanie komunikatu błędu w systemie monitorującym
- i. usunąć sabotaż
- j. ponowić wysyłkę
- k. komunikat błędu w systemie monitorującym powinien zostać rozwiązany

II Wyświetlenie dynamicznej wizualizacji danych z monitoringu

- 6 Zalogować się do systemu jako administrator.
- 7 Utworzyć dedykowany **Widok1** w ramach dedykowanego pulpitu zawierający wykres prezentujący użycie procesora i użycie pamięci w ciągu ostatnich 10 min.
- 8 Utworzyć dedykowany **Widok2** zawierający wykres prezentujący użycie interfejsu sieciowego w ciągu ostatnich 10 min (bity wysłane i odebrane).
- 9 Zapisać zmiany w widokach i zweryfikować odświeżanie danych na wykresach.

III Zarządzanie powiadomieniami

- 10 Zalogować się do systemu jako administrator.
- 11 Przejść do konfiguracji powiadomień, zweryfikować dostępność schematów powiadomień dla następujących sposobów komunikacji: Email, SMS.
- Zweryfikować poprawność wysyłki wiadomości powiadomień przez system.

IV Zarządzanie użytkownikami

- 12 Zalogować się do systemu jako administrator.
- 13 Zdefiniować politykę haseł dla użytkownika wymagającą stosowanie:
 - a. min. długość 16 znaków
 - b. zawierającego co najmniej jedną wielką i małą literę alfabetu łacińskiego
 - c. cyfrę
 - d. znak specjalny
 - e. nie może zawierać imienia, nazwiska, nazwy użytkownika
- 14 Utworzyć grupy przywilejów:
 - a. pierwszą umożliwiającą odczyt wszystkich danych z obiektów dodanych w kroku 2 i 3
 - b. drugą umożliwiającą wyświetlenie danych z dedykowanego pulpitu
- 15 Utworzyć nowe konto użytkownika.
- 16 Nadać uprawnienia do widoku powstałego w punkcie 7.
- 17 Utworzyć grupę przywilejów umożliwiającą odczyt wszystkich danych z obiektów dodanych w punkcie 7 do pulpitu.
- 18 Zalogować się na konta Użytkowników i zaprezentować różnice.

V Funkcjonalność raportów

- 19 Zalogować się do systemu jako administrator.
- 20 Zademonstrować Log audytu systemu.
- 21 Zademonstrować raport dostępności usług.