Zblewo, dn. 21.11.2024 r.

Nr sprawy: RO.271.30.2024

Specyfikacja Warunków Zamówienia

na wykonanie zadania:

Dostawa sprzętu i oprogramowania wraz z usługą wdrożenia realizowana 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: Artur Marcin Herold; Wójt Gminy Zblewo

Elektronicznie podpisany przez Artur Marcin Herold; Wójt Gminy Zblewo
Data: 2024.11.21 11:03:01 +01'00'

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Spis treści

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

ROZDZIAŁ 1.
INFORMACJE O ZAMAWIAJĄCYM

Nazwa: Gmina Zblewo
Adres: 83-210 Zblewo ul. Główna 40
Numer telefonu: 585884381
Adres strony internetowej: www.zblewo.pl
Adres poczty elektronicznej: gmina@zblewo.pl
Adres skrzynki ePUAP**:** /2359bfvitd/SkrytkaESP
Godziny urzędowania: poniedziałek - od 7.30 do 16.00, wtorek - od 7.30 do 15.30, środa - od 7.30 do 16.00, czwartek - od 7.30 do 15.00, piątek - od 7.30 do 15.00
Adres strony internetowej prowadzonego postępowania: **https://platformazakupowa.pl/pn/zblewo**

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 składania 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 stronie internetowej prowadzonego postępowania za pośrednictwem platformazakupowa.pl pod adresem: https://platformazakupowa.pl/pn/zblewo 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".

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

ROZDZIAŁ 3.
OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest **Dostawa sprzętu i oprogramowania wraz z usługą wdrożenia** realizowane w ramach projektu grantowego „Cyberbezpieczny Samorząd”.

LP.	OPIS
CZĘŚĆ 1	
1.	System NDR (Network Detection and Response)
CZĘŚĆ 2	
1.	Rozbudowa zabezpieczeń logicznych (firewall) – zakup UTM
CZĘŚĆ 3	
1.	Wirtualny serwer do zbierania i przechowywania logów systemowych
CZĘŚĆ 4	
1.	Serwer do systemu zbierania logów krytycznych
CZĘŚĆ 5	
1.	Oprogramowanie umożliwiające monitoring usług i użytkowanych systemów

2. Szczegółowy zakres zamówienia:

<u>CZĘŚĆ 1</u> System NDR (Network Detection and Response)

Dostawa oraz wdrożenie urządzenia klasy NDR (Network Detection and Response) wraz z oprogramowaniem

Minimalne parametry techniczne i funkcjonalne:
Elementy systemu bezpieczeństwa

a. Wysokość 1U do montażu w szafie rack.
b. Posiadać co najmniej dwa porty USB
c. Urządzenie musi posiadać dedykowany port do zarządzania
d. Urządzenie musi posiadać minimum interfejsów: 2x SFP+, 8x SFP, 8x GE
e. Musi obsługiwać co najmniej 1T przestrzeni dyskowej.
f. Minimum 1 Gb/s przepustowości wykrywania naruszeń w dwukierunkowym ruchu HTTP z włączonymi wszystkimi funkcjami wykrywania zagrożeń
g. Proponowane rozwiązanie musi obsługiwać minimum 750 tys . jednoczesnych sesji.
h. Proponowane rozwiązanie musi obsługiwać 32000 nowych sesji /s w ruchu HTTP.

Usługi sieciowe

a. Musi obsługiwać pasywny tryb pracy (TAP), nie ingerując w sieć klienta.
b. Rozwiązanie musi być w stanie zintegrować się z zaporami ogniowymi tej samej marki w celu ograniczenia zagrożeń.
c. Musi posiadać możliwość rozwiązywania wiadomości przez protokół MPLS, VXLAN oraz QinQ i wykrywania zagrożeń w tych wiadomościach.

Kontrola aplikacji

a. Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka oraz wspierać komunikatory internetowe, p2p, pocztę e-mail, przesyłanie plików, gry online, strumieniowe przesyłanie multimediów itp.
b. Rozwiązanie musi być w stanie zidentyfikować aplikacje mobilne typu iOS lub Android.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

c. Rozwiązanie musi być w stanie identyfikować aplikacje w chmurze, musi zapewniać wielowymiarowe monitorowanie i statystyki dla aplikacji w chmurze, w tym kategorię ryzyka i funkcje.

Wykrywanie zagrożeń

a. Rozwiązanie musi obsługiwać co najmniej 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, ręczne i automatyczne aktualizacje, wyodrębnianie sygnatur oraz wbudowaną encyklopedię zagrożeń.
b. Rozwiązanie musi obsługiwać ochronę przed atakami SQL injection, XSS, buffer overflow zarówno dla IPv4 jak i IPv6
c. Rozwiązanie powinno obsługiwać ochronę przez atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, Musi obsługiwać wykrywanie co najmniej metod uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA
d. Rozwiązanie musi obsługiwać wykrywanie anomalii protokołów HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS itp.
e. Niestandardowe reguły wykrywania włamań muszą obsługiwać konfigurowanie kierunku ruchu ataku w celu poprawy dokładności analizy źródła ataku.
f. Rozwiązanie powinno umożliwiać tworzenie białych list dla modułu IPS.
g. Rozwiązanie musi mieć wstępnie zdefiniowane profile IPS.
h. Rozwiązanie musi mieć opcję przechwytywania pakietów
i. Rozwiązanie musi umieć wykrywa reverse-shell
j. Rozwiązanie potrafi zdefiniować odpowiednie treshholdy chroniące przed atakami Flood, bazując na parametrach dostarczonego ruchu
k. System musi mapować wykryte zagrożenia na framework MITRE ATT&CK

Skanowanie antywirusowe

a. Rozwiązanie musi obsługiwać co najmniej 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur.
b. Rozwiązanie musi wspierać antywirus oparty na przepływie dla protokołów min. HTTP, SMTP, POP3, IMAP, FTP/SFTP.
c. Rozwiązanie powinno obsługiwać wykrywanie wirusów w skompresowanych plikach, takich jak RAR, ZIP, GZIP, BZIP2, TAR oraz wspierać. wielowarstwowe wykrywanie skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji po wykryciu zagrożenia w tych plikach.
d. Rozwiązanie musi obsługiwać wykrywanie zaszyfrowanych skompresowanych plików.

Wykrywanie botnetów C&C

a. Rozwiązanie powinno wspierać skuteczne wykrywanie botów intranetowych i zapobieganie dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównywanie uzyskanych informacji z bazą adresów C&C.
b. Rozwiązanie musi obsługiwać automatyczną aktualizację sygnatur botnetów C&C
c. Rozwiązanie musi obsługiwać dwa typy bazy adresów C&C: bazę adresów IP i bazę danych domen.
d. Rozwiązanie musi obsługiwać wykrywanie C&C protokołów w protokołach TCP, HTTP i DNS.
e. Rozwiązanie musi wspierać właczenie wykrywania DGA w celu analizy odpowiedzi DNS i wykrywania, czy urządzenie jest atakowane przez nazwę domeny DGA.
f. Musi wspierać wykrywanie tunelowania w protokole DNS w tym analizowanie zapytań DNS a także rejestrować logów zagrożeń wykrytych tuneli DNS.

Sandbox w chmurze

a. Rozwiązanie musi obsługiwać oparte na chmurze wirtualne środowisko analizy złośliwego oprogramowania w celu znalezienia nieznanych zagrożeń
b. Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do piaskownicy w chmurze w celu analizy.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

c. Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów, w tym HTTP/HTTPS, POP3, IMAP4, SMTP i FTP.
d. Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR , SWF oraz skrypty
e. Rozwiązanie powinno dostarczyć kompletny raport analizy behawioralnej dla złośliwych plików.
f. Rozwiązanie musi obsługiwać globalne udostępnianie informacji o zagrożeniach, aby wykryć nowe nieznane zagrożenie.

Wykrywanie spamu
a. Rozwiązanie musi wspierać klasyfikację i wykrywanie spamu w czasie rzeczywistym
b. Rozwiązanie musi obsługiwać wykrywanie spamu niezależnie od języka, formatu lub treści wiadomości.
c. Rozwiązanie musi obsługiwać protokoły poczty e-mail smtp i pop3
d. Rozwiązanie musi obsługiwać białe listy wiadomości e-mail z zaufanych domen.

Dodatkowe funkcje ochrony
a. Rozwiązanie musi obsługiwać wykrywanie DoS / DDoS, SYN Flood, DNS query flood itp.
b. Rozwiązanie musi obsługiwać wykrywanie ataków ARP w tym spoofing ARP
c. Rozwiązanie musi obsługiwać wykrywanie anormalnych ataków protokołu.
d. Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu pop

Inteligentne funkcje bezpieczeństwa
a. Rozwiązanie powinno obsługiwać analizę korelacji zagrożeń, korelację między nieznanymi zagrożeniami, nietypowym zachowaniem i zachowaniem aplikacji, aby wykryć potencjalne zagrożenia lub ataki.
b. Rozwiązanie powinno umożliwiać aktualizację bazy danych modelu zachowania szkodliwego oprogramowania online w czasie rzeczywistym.
c. Rozwiązanie powinno obsługiwać wykrywanie ponad 2000 znanych i nieznanych rodzin złośliwego oprogramowania, w tym wirusów, robaków, trojanów itp.
d. Rozwiązanie musi obsługiwać zaawansowane wykrywanie złośliwego oprogramowania oparte na obserwacji zachowania
e. Rozwiązanie musi wspierać wykrycia oprogramowania ransomware i złośliwego oprogramowania do wydobywania kryptowalut.
f. Rozwiązanie powinno obsługiwać modelowanie zachowania w oparciu o ruch bazowy L3-L7, aby ujawnić nietypowe zachowanie sieci, takie jak skanowanie HTTP, Spider, SPAM, słabe hasła SSH / FTP dla serwerów i hostów.
g. Rozwiązanie musi obsługiwać wykrywanie DDoS, w tym Flood, Sockstress, zip of death, reflect, dns query, SSL DDos i aplikacyjny DDoS
h. Rozwiązanie musi obsługiwać inspekcję zaszyfrowanego ruchu tunelowego dla nieznanych aplikacji
i. Rozwiązanie musi obsługiwać aktualizację bazy danych modelu nieprawidłowego zachowania online w czasie rzeczywistym
j. Rozwiązanie musi zapewniać analizę kryminalistyczną , w tym analizę zagrożeń, bazę wiedzy, historię i topologię zagrożeń.
k. Rozwiązanie musi obsługiwać działania administratora w celu zmiany stanu zagrożenia na false positive, naprawionego, zignorowanego, potwierdzonego zdarzenia
l. Rozwiązanie musi obsługiwać czyszczenie zagrożeń serwera jednym kliknięciem i ponowną ocenę bezpieczeństwa hosta
m. Rozwiązanie powinno obsługiwać białą listę zagrożeń, w tym nazwę zagrożenia, źródłowy/docelowy adres IP, liczbę odwiedzin itd.
n. Rozwiązanie musi obsługiwać przechwytywanie pakietów online

o. Rozwiązanie musi obsługiwać lokalną technologię honeypot, aby wychwytywać ataki zagrożeń sieciowych i potwierdzać źródło zagrożenia, typ zagrożenia i częstość występowania
p. Rozwiązanie musi obsługiwać wykrywanie oszustw na podstawie behawioralnej dla ftp, HTTP, MYSQL, SSH, TELNET, dokumentów lub baz danych
q. Rozwiązanie musi obsługiwać funkcję polowania na zagrożenia (threat hunting), aby zebrać kompleksowe dowody i zapewnić dogłębną analizę
r. Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force remote dekto, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu poprawy wykrywalność funkcji śledzenia zagrożeń.

Widoczność ryzyka/zagrożeń

a. Rozwiązanie musi obsługiwać wizualizację zagrożeń intranetowych dla serwerów (zasobów krytycznych), a także wykrywanie nietypowego ruchu z nimi związanego.
b. Rozwiązanie musi obsługiwać widoczność zagrożeń dla ryzykownych hostów, w tym nazwy hosta, systemu operacyjnego, przeglądarki, typu usługi, aby rejestrować zagrożenia hosta i nietypowy ruch.
c. Rozwiązanie musi obsługiwać widoczność podstawowych informacji opartych na hoście, indeksu ryzyka, zagrożeń i nietypowego ruchu.
d. Rozwiązanie powinno wspierać widoczność zagrożeń, w tym nazwę zagrożenia, typ zagrożenia, poziom ryzyka, bazę wiedzy, pakiet kryminalistyczny itp.
e. Rozwiązanie powinno dostarczyć wszystkie statystyki klasyfikacji zdarzeń zagrożeń w oparciu o IOC i trend zdarzeń zagrożeń w ciągu co najmniej 2 tygodni.
f. Rozwiązanie musi wspierać wskazanie ścieżki ataku.

Analiza i odpowiedzi na incydenty

a. Rozwiązanie musi obsługiwać aktualizację w czasie rzeczywistym najpoważniejszych informacji o zagrożeniach znalezionych w branży do urządzenia z chmury
b. Obsługa wyświetlania najnowszych informacji o zagrożeniach w wyskakujących okienkach.
c. Obsługa rejestrowania i sprawdzania, czy w sieci wystąpiło odpowiednie zagrożenie.
d. Pomoc techniczna w celu dostarczenia szczegółowych informacji o zagrożeniach i sugestii dotyczących rozwiązania.
e. Wsparcie konfigurowania reguł ostrzegania o zagrożeniach, w tym warunków zagrożenia i metody działania, które w przypadku wystąpienia zdarzenia stanowiącego zagrożenie, system powiadomi użytkownika lub podejmie odpwiedź w odpowiednim czasie zgodnie z metodą działania określoną w regule (np. połączenie z firewall, przypomnienie głosowe lub wysłanie pocztą e-mail.

Administracja

a. Rozwiązanie musi mieć zintegrowany sieciowy interfejs użytkownika (WebUI) i interfejs wiersza poleceń (CLI)
b. Rozwiązanie powinno obsługiwać zarządzanie dostępem z HTTP/HTTPS, SSH, telnet, konsoli
c. Rozwiązanie musi być w stanie chronić system przed atakami brute-force na nazwę użytkownika i hasło
d. Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów.
e. Rozwiązanie musi obsługiwać monitorowanie hostów i serwerów w sieci wewnętrznej, identyfikując nazwę, system operacyjny, przeglądarkę, typ i rejestr statystyk zagrożeń sieciowych
f. Oferowany zestaw urządzeń musi pochodzić o jednego producenta i być w pełni kompatybilny
g. Oferowany zestaw urządzeń musi posiadać aplikację mobilną pozwalającą na monitoring pracy urządzeń i analizę zdarzeń

Logowanie i raportowanie

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

a. Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. Raport można wyeksportować co najmniej w formacie PDF i/lub wysłać na adres e-mail lub FTP.
b. Rozwiązanie powinno obsługiwać ustawianie alarmów dotyczących wykorzystania procesora, wykorzystania pamięci, wykorzystania miejsca na dysku, nowych połączeń itp.
c. Rozwiązanie powinno obsługiwać wysyłanie alarmów przez e-mail, SMS.
d. Alerty powinny być generowane na podstawie przepustowości aplikacji i nowych połączeń.
e. Logi powinny być możliwe do eksportu za pośrednictwem Syslog lub poczty e-mail i zawierać minimum logi zdarzeń, sieci, zagrożenia, konfigurację i sesje
f. Wstępnie zdefiniowane zadania raportowania
g. Rozwiązanie powinno mieć scentralizowane monitorowanie wielu urządzeń, w tym procesora, pamięci, ruchu, sesji, aplikacji, użytkowników, zagrożeń itp. za pośrednictwem aplikacji mobilnej z danymi z ostatnich 7 dni.
h. Rozwiązanie musi wspierać restAPI.

Wymagania dotyczące dostawy oraz gwarancji sprzętu:
a. Sprzęt musi być objęty 24-miesięczną gwarancją producenta, ze wspraciem technicznym dostępnym przez 24 godziny przez 7 dni w tygodniu.
b. Sprzęt musi posiadać licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 24 miesięcy (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C)
c. Wsparcie techniczne dystrybutora rozwiązań w języku polskim.
d. Wdrożenie musi zostać zrealizowane przez wykonawcę, który posiada co najmniej 2 certyfikaty wydane przed producenta rozwiązania świadczące o posiadanych kompetencjach do prawidłowego wykonania usługi.
e. Dostawca musi zapewnić rozszerzone wsparcie techniczne obejmujące 12 godzin konsultacji technicznych z możliwością zdalnej pomocy przy konfiguracji urządzenia.

Szkolenie specjalistycznie dla administratorów:
a. Zostanie przeprowadzone przez Wykonawcę w siedzibie Zamawiającego, dla 2 pracowników Zamawiającego
b. Szkolenie potrwa 1 dzień roboczy przez min. 6 godzin.
c. Szkolenie zostanie przeprowadzone w formie warsztatów przez dostawcę posiadającego odpowiednie kompetencje potwierdzone certyfikatem producenta rozwiązania.

Dostawa oraz wdrożenie urządzenia klasy NIPS (Network Intrusion Prevention System) wraz z oprogramowaniem (1 szt.).

Minimalne parametry techniczne i funkcjonalne:
Elementy systemu bezpieczeństwa
a. Proponowane rozwiązanie powinno mieć maksymalną wysokość 1U.
b. Proponowane rozwiązanie musi posiadać co najmniej dwa porty USB.
c. Proponowane rozwiązanie musi posiadać co najmniej jeden port konsoli
d. Proponowane rozwiązanie musi posiadać co najmniej jeden dedykowany port do zarządzania systemem
e. Proponowane rozwiązanie musi posiadać co najmniej 8 stałych portów Gigabit Ethernet.
f. Proponowane rozwiązanie musi posiadać co najmniej 8 stałych portów SFP.
g. Proponowane rozwiązanie musi posiadać co najmniej 2 stałe porty SFP+.
h. Proponowane rozwiązanie musi posiadać co najmniej 480GB przestrzeni dyskowej.
i. Proponowane rozwiązanie musi obsługiwać przepustowość IPS 3 Gb/s
j. Proponowane rozwiązanie musi obsługiwać jednoczesne sesje o długości 1.2 M

k. Proponowane rozwiązanie musi obsługiwać min 40000 nowych sesji/sekundę w ruchu HTTP, z włączonym silnikiem IPS.
l. Opóźnienia (tzw. Latency) nie mogę przekraczać 300µs
m. Funkcjonalności nie mogą być realizowane na rozwiązaniu NGFW
n. Usługi sieciowe
Proponowane rozwiązanie musi być w stanie pracować jednocześnie w trybie warstwy 3 (routing), trybie online (most) i warstwie 2 (kopia ruchu) (bez konieczności wirtualizacji sprzętu)

Kontrola Aplikacji

a. Rozwiązanie powinno obsługiwać identyfikację IP hostów, ilość endpointów , czasu online, czasu offline.
b. Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka.
c. Rozwiązanie powinno rozpoznawać aplikacje IPv6.
d. Rozwiązanie musi obsługiwać identyfikację aplikacji dla ruchu szyfrowanego SSL
e. Rozwiązanie musi wspierać identyfikację aplikacji mobilnych na Androida i iOS.
f. Rozwiązanie powinno obsługiwać wyświetlanie opisu, czynników ryzyka, zależności, typowych używanych portów i adresów URL dla dodatkowych odwołań i informacji dla każdej aplikacji w interfejsie WebUI.
g. Rozwiązanie musi obsługiwać blokowanie, ponowne uruchamianie sesji, monitorowanie i kształtowanie ruchu dla aplikacji.
h. Rozwiązanie musi być w stanie identyfikować i kontrolować aplikacje w chmurze

Ochrona przez zagrożeniami

a. Rozwiązanie musi obsługiwać ponad 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, automatyczne wstawianie lub wyodrębnianie sygnatur oraz zintegrowaną encyklopedię zagrożeń.
b. Rozwiązanie musi obsługiwać zapobieganie włamaniom dla ruchu szyfrowanego SSL.
c. Rozwiązanie musi obsługiwać ochronę środowiska IPV6.
d. Rozwiązanie musi obsługiwać ochronę przed sql injection, CC i atakom XSS.
e. Rozwiązanie musi obsługiwać sprawdzanie linków zewnętrznych.
f. Rozwiązanie powinno obsługiwać ochronę przed atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, metodami przyjaznymi dla robotów. Wspierane powinny być 4 metody uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA
g. Rozwiązanie powinno obsługiwać wykrywanie anomalii protokołu.
h. Rozwiązanie musi obsługiwać następujące akcje IPS: monitorowanie, blokowanie, resetowanie (adres IP atakujących lub IP ofiary, interfejs wejściowy) z czasem wygaśnięcia
i. Rozwiązanie musi obsługiwać opcję logowania pakietów.
j. Rozwiązanie musi obsługiwać profil zabezpieczeń IPS na podstawie ważności, obiektu docelowego, systemu operacyjnego, aplikacji lub protokołu.
k. Rozwiązanie musi obsługiwać zapobieganie włamaniom dla protokołów HTTP, SMTP, IMAP. POP3, VOIP, NETBIOS itp.
l. Rozwiązanie musi być wspierać weryfikację protokołów http typu Get, Head, Put, Post.
m. Rozwiązanie musi obsługiwać wyłączenie IP z określonych sygnatur IPS.
n. Rozwiązanie musi obsługiwać tryb działania sniffera IDS.
o. Rozwiązanie musi obsługiwać predefiniowaną konfigurację profili IPS.
p. Rozwiązanie musi obsługiwać tworzenie zdefiniowanych przez użytkownika sygnatur IPS.
q. Proponowane rozwiązanie musi obsługiwać wykrywanie reputacji IP i blokowanie adresów IP serwera botnetów za pomocą globalnej bazy danych reputacji IP.
r. Proponowane rozwiązanie powinno wspierać szczegółowy opis predefiniowanych profili IPS.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

s. Rozwiązanie musi obsługiwać rejestrację zagrożeń IPv6: obsługa przechwytywania i pobierania pakietów IPv6
t. Szczegóły zagrożeń muszą obsługiwać identyfikator URI i dekodowanie danych ataków
u. Obsługa wykrywania anomalii protokołów HTTP/DNS/FTP/MSRPC/POP3/SMTP/SUNRPC i Telnet
v. Obsługa inspekcji Reverse Shell
w. Blokowanie plików po rozszerzeniu dla minimum 100 typów plików
x. Rozwiązanie musi wykrywać i blokować wrażliwe zrefowanych informacje w przesyłanych plikach dla minimum doc/docx, xls/xlsx, ppt/pptx, txt w protokołach HTTP, FTP, SMTP, POP3, IMAP, SMB
y. Ochrona i wykrywanie skanowania protokołow IP oraz UDP
z. Rozwiązanie musi mieć możliwość inspekcji payloudu w ramkach MPLS
aa. Rozwiązanie pozwala na automatyczne określanie wartości proponowanych dla ochrony przed atakami Flood
bb. System pozwala na zdefiniowanie globalnej białej listy, pozwalając na dany ruch i nie sprawdzając go na warstwie aplikacyjnej
cc. System musi mapować wykryte zagrożenia na taktyki MITRE ATT&CK

Antywirus

a. Rozwiązanie musi obsługiwać ponad 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur.
b. Rozwiązanie musi obsługiwać antywirus oparty na przepływie dla protokołów HTTP, SMTP, POP3, IMAP, FTP/SFTP, SMB
c. Rozwiązanie powinno obsługiwać wykrywanie wirusów dla skompresowanych plików, takich jak RAR, ZIP, GZIP, BZIP2, TAR; obsługa wielowarstwowego wykrywania skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji
d. Rozwiązanie musi obsługiwać akcje niestandardowe dla zaszyfrowanych plików skompresowanych.
e. Rozwiązanie musi obsługiwać co najmniej 3 działania: usuwanie złośliwego kodu, resetowanie połączenia lub logowanie tylko po wykryciu wirusa lub złośliwej strony internetowej
f. Rozwiązanie powinno obsługiwać ostrzeganie przed wirusami i złośliwymi stronami internetowymi, ostrzegać użytkownika, że witryna jest szkodliwą witryną lub że wykryto wirusa.
g. Rozwiązanie musi obsługiwać funkcje AV w środowiskach IPV6.

Filtrowanie adresów URL

a. Rozwiązanie musi obsługiwać dynamiczne filtrowanie sieci Web za pomocą chmurowej bazy danych kategoryzacji w czasie rzeczywistym: ponad 140 milionów adresów URL z co najmniej 64 kategoriami (z których nie mniej niż 8 jest związanych z bezpieczeństwem)
b. Rozwiązanie musi obsługiwać ręcznie zdefiniowane filtrowanie sieci Web na podstawie adresu URL, zawartości sieci Web i nagłówka MIME
c. Rozwiązanie musi obsługiwać następujące dodatkowe funkcje filtrowania.
   - Aplet Java, ActiveX lub filtr plików cookie.
   - Blokowanie postów http
   - Rejestrowanie wyszukiwania słów kluczowych
   - Wykluczanie ze skanowania połączeń szyfrowanych w niektórych kategoriach dla prywatności.
d. Rozwiązanie musi obsługiwać zastępowanie profilu filtrowania adresów URL, aby administrator mógł tymczasowo przypisać różne profile do użytkownika/grupy/adresu IP
e. Rozwiązaniem powinno być umożliwienie dostosowania strony ostrzeżenia do filtrowania adresów URL.

Sandbox

a. Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do chmury w celu analizy

b. Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów takich jak HTTP/HTTPS, POP3, IMAP, SMTP, FTP i SMB
c. Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR , SWF i Skryptów
d. Rozwiązanie musi obsługiwać kierunek transferu plików i kontrolę rozmiaru pliku.
e. Rozwiązanie musi zawierać kompletny raport analizy zachowania złośliwych plików
f. Rozwiązanie powinno obsługiwać blokowanie zgodnie z wynikami wykrywania, aby szybko zablokować nieznane zagrożenie.
g. Rozwiązanie musi obsługiwać udostępnianie globalnych informacji o zagrożeniach i blokować nieznane zagrożeni na całym świecie

Zapobieganie C&C i botnetom

a. Rozwiązanie musi być w stanie skutecznie wykrywać boty intranetowe i zapobiegać dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównanie uzyskanych informacji z bazą adresów C&C
b. Rozwiązanie musi obsługiwać regularne aktualizacje adresów serwerów botnetu.
c. Rozwiązanie musi obsługiwać dwa typy bazy danych adresów C&C: bazę danych adresów IP (z wyłączeniem adresów IPv6) i bazę danych domen
d. Rozwiązanie musi obsługiwać wykrywanie dla protokołów TCP, HTTP i DNS.
e. Rozwiązanie musi obsługiwać ręczne umieszczanie adresów IP i domen na białej liście.
f. Rozwiązanie musi umożliwiać ręczny import/eksport i automatyczny import czarnych list
g. Rozwiązanie musi obsługiwać funkcjonalność DNS Sinkhole i wykrywanie tunelowania DNS.

Monitoring

a. Rozwiązanie musi posiadać pełne monitorowanie zagrożeń, w tym nazwę ataku, ważność, czasem, adresem, protokołem, zalecanym rozwiązaniem itp.
b. Rozwiązanie musi obsługiwać usługę Threat Intelligence Pushing Service
c. Rozwiązanie musi obsługiwać statystyki i analizy ruchu w czasie rzeczywistym.
d. Rozwiązanie powinno obsługiwać monitorowanie stanu procesora, pamięci, temperatury, wentylatora, modułów zasilania itp.

Polityki bezpieczeństwa

a. Proponowane rozwiązanie musi obsługiwać kontrolę dostępu do strefy (zone), użytkownika, usługi, aplikacji, IPS, AV w jednej regule polityki.
b. Proponowane rozwiązanie musi obsługiwać wstępnie zdefiniowane i niestandardowe obiekty
c. Proponowane rozwiązanie musi obsługiwać weryfikację nadmiarowości polityki bezpieczeństwa oraz zliczanie trafień polityki przez interfejs WebUI
d. Rozwiązanie musi obsługiwać import i eksport polityk

Administrowanie, logi i raportowanie

a. Rozwiązanie musi być obsługiwane przez WebUI i interfejs wiersza poleceń (CLI)
b. Rozwiązanie powinno obsługiwać zarządzanie dostępem przez HTTP/HTTPS, SSH, telnet, konsolę
c. Rozwiązanie musi obsługiwać uwierzytelnianie dwuskładnikowe: nazwa użytkownika/hasło, plik certyfikatu HTTPS
d. Rozwiązanie musi obsługiwać integrację systemu: SNMP, syslog.
e. Rozwiązanie musi obsługiwać co najmniej 3 role administratora, w tym administratora, operatora i audytora
f. Rozwiązanie musi być w stanie chronić system przed atakami brute force na nazwę użytkownika i hasło
g. Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów.
h. Rozwiązanie musi obsługiwać serwery Radius, AD i LDAP.

i. Rozwiązanie musi obsługiwać szybkie wdrażanie poprzez automatyczne instalowanie z USB, uruchamianie skryptów lokalnych i zdalnych.
j. Rozwiązanie musi obsługiwać dynamiczny dashboard w czasie rzeczywistym i szczegółowe widżety monitorowania
k. Urządzenie musi obsługiwać zarządzanie urządzeniami pamięci masowej: dostosowywanie i alarmowanie progu przestrzeni dyskowej, nakładanie starych danych, zatrzymywanie nagrywania ruchu.
l. Urządzenie musi obsługiwać szczegółowe logi ruchu: przekazane, sesje naruszone, ruch lokalny, nieprawidłowe pakiety
m. Urządzenie musi obsługiwać pełne logi zdarzeń: audyty aktywności systemu i zarządzania, routing i sieć, VPN, uwierzytelnianie użytkowników, zdarzenia związane z Wi-Fi
n. Urządzenie musi obsługiwać opcję rozpoznawania nazw portów usług i adresów IP.
o. Rozwiązanie musi mieć możliwość dodania adresów IP lub MAC hostów do czarnej listy, aby zablokować dostęp przez określony czas.
p. Rozwiązanie powinno obsługiwać blokowanie konta po kilku niepowodzeniach logowania.
q. Rozwiązanie musi obsługiwać konfigurację zadań przechwytywania pakietów z wieloma warunkami przechwytywania pakietów w tym samym czasie oraz ich export
r. Rozwiązanie musi obsługiwać standardowy SYSLOG i logowanie w formacie binarnym; rozproszone binarne przechowywanie logów na wielu serwerach logów
s. Rozwiązanie powinno obsługiwać logowanie w pamięci lokalnej i/lub serwerach syslog.
t. Rozwiązanie musi obsługiwać rejestrowanie zmiany w politykach
u. Rozwiązanie musi obsługiwać logowanie zaufane przy użyciu opcji TCP (RFC 3195)
v. Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika.
w. Rozwiązanie musi obsługiwać zaplanowany raport.
x. Raport można wyeksportować w formacie PDF/HTML/WORD za pośrednictwem email lub FTP.
y. Rozwiązanie musi umożliwić podgląd raportów w formacie HTML i PDF.

Wysoka dostępność

a. Rozwiązanie musi obsługiwać tryby Active/Active i Active/Passive
b. Rozwiązanie musi obsługiwać następujące opcje wdrażania HA:- HA z agregacją linków
   - Full mesh HA
   - Geograficznie rozproszony HA
c. Rozwiązanie musi obsługiwać funkcję bypass sprzętowych interfejsów i dedykowany interfejs HA QoS
d. Rozwiązanie musi obsługiwać maksymalną lub gwarantowaną kontrolę przepustowości dla adresów IP lub użytkowników.
e. Rozwiązanie powinno obsługiwać tunelowanie w oparciu o domenę zabezpieczeń, interfejs, adres, pulę użytkowników/użytkowników, pulę serwer/serwer, pulę aplikacji/aplikacji, TOS, sieci VLAN.
f. Rozwiązanie musi obsługiwać przepustowość przydzieloną w zakresie - czas, priorytet lub tę samą współdzieloną przepustowość
g. Rozwiązanie musi obsługiwać typ usługi (TOS) i zróżnicowane usługi (DiffServ)
h. Rozwiązanie musi obsługiwać tworzenie zaplanowanych polityk QoS.
i. Rozwiązanie musi obsługiwać elastyczną, priorytetową alokację pozostałej niewykorzystanej przepustowości.
j. Rozwiązanie musi obsługiwać dwa poziomy konfiguracji ruchu, które umożliwiają konfigurację ruchu w różnych wymiarach, takich jak użytkownicy i aplikacje. Rozwiązanie musi obsługiwać co najmniej cztery tunele na poziom, co zapewnia hierarchię kontroli ruchu.
k. Rozwiązanie musi obsługiwać alokację przepustowości na podstawie kategorii adresu URL
l. Rozwiązanie musi obsługiwać adresy IPv6 w funkcji QoS.

Ochrona przed spamem

a. Rozwiązanie musi obsługiwać klasyfikację spamu w czasie rzeczywistym i zapobieganie mu.
b. Rozwiązanie musi obsługiwać ochronę niezależnie od języka, formatu lub zawartości wiadomości.
c. Rozwiązanie musi obsługiwać protokoły poczty e-mail SMTP i POP3.
d. Rozwiązanie musi obsługiwać wykrywanie zarówno ruchu przychodzącego, jak i wychodzącego.
e. Rozwiązanie musi obsługiwać białe listy, aby umożliwić wysyłanie wiadomości e-mail z zaufanych domen.
f. Rozwiązanie musi obsługiwać listę obejść opartą na nadawcy i niestandardowe reguły spamu.
g. Rozwiązanie musi mieć możliwość konfiguracji czarnych i białych list dla modułu Anti-Spam.

Reputacja IP

a. Obsługa filtrowania ruchu z adresów IP o niskiej reputacji, w tym botnetów, spamu, węzłów Tora, skompromitowanych, Brute-force itp.
b. Obsługa rejestrowania, usuwania lub blokowania pakietów, jeśli złośliwy ruch dotrze do listy reputacji IP.
c. Obsługa uaktualniania bazy danych przez zainstalowanie licencji IP Reputation.
d. Obsługa filtrowania adresów IP botów.

Wymagania dotyczące dostawy oraz gwarancji sprzętu:

a. Gwarancja producenta i wsparcie techniczne - nie później niż do 30.06.2026r., ze wsparciem technicznym dostępnym przez 24 godziny przez 7 dni w tygodniu.
b. Sprzęt musi być objęty rozszerzonym wsparciem technicznym – gwarantującym w przypadku awarii – wymianę lub naprawę urządzenia w ciągu 24 godzin od wcześniejszego poinformowania Dostawcy przez wysłaną wiadomość na wskazany do komunikacji adres e-mail w dniach roboczych.
c. Sprzęt musi posiadać licencje na wszystkie funkcje bezpieczeństwa producentów na okres nie później niż do 30.06.2026r. (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C)
d. Wsparcie techniczne dystrybutora rozwiązań w języku polskim
e. Wdrożenie musi zostać zrealizowane przez wykonawcę, który posiada co najmniej 2 certyfikaty wydane przed producenta rozwiązania świadczące o posiadanych kompetencjach do prawidłowego wykonania usługi.

Szkolenie specjalistycznie dla administratorów:

a. Zostanie przeprowadzone przez Wykonawcę w siedzibie Zamawiającego, dla 2 pracowników Zamawiającego.
b. Szkolenie potrwa 1 dzień roboczy przez min. 6 godzin.
c. Szkolenie zostanie przeprowadzone w formie warsztatów przez dostawcę posiadajacego odpowiednie kompetencje potwierdzone certyfikatem producenta rozwiązania.

<u>CZĘŚĆ 2</u> Rozbudowa zabezpieczeń logicznych (firewall) – zakup UTM

Obsługa sieci

Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

Zapora korporacyjna (Firewall)

a. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
b. Urządzenie ma obsługiwać translacje adresów NAT n:l, NAT 1:1 oraz PAT.
c. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

d. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
e. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
f. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
g. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
h. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
i. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
j. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
k. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

Intrusion Prevention System (IPS)

a. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
b. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
c. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
d. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
e. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
f. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
g. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
h. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
i. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
j. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

Kształtowanie pasma (Traffic Shapping)

a. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.

b. Ograniczenie pasma lub priorytetyzacja reguły fi rewa II ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
c. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
d. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

Ochrona antywirusowa

a. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
b. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
c. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
d. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

Ochrona antyspam

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

Wirtualne sieci prywatne (VPN)

a. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny - lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
b. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
   - PPTP VPN,
   - IPSec VPN,
   - SSL VPN.
c. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
d. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
e. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
f. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
g. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
h. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

Filtr dostępu do stron www

a. Urządzenie ma posiadać wbudowany filtr URL.
b. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
c. Administrator ma mieć możliwość dodawania własnych kategorii URL.

d. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
e. blokowanie dostępu do adresu URL,
f. zezwolenie na dostęp do adresu URL,
g. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
h. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
i. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
j. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
k. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
l. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
m. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

Uwierzytelnianie

a. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
   - lokalną bazę użytkowników (wewnętrzny LDAP),
   - zewnętrzną bazę użytkowników (zewnętrzny LDAP),
   - usługę katalogową Microsoft Active Directory.
b. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
c. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
   - SSL,
   - Radius,
   - Kerberos.
d. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
e. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
f. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
g. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
h. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
i. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.

Administracja łączami do internetu (ISP)

a. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
b. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
   - równoważenie względem adresu źródłowego,
   - równoważenie względem połączenia.
c. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
d. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

e. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
f. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
g. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

Routing (trasowanie)

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

Administracja urządzeniem

a. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
b. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
c. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
d. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
e. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
f. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
g. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
h. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
i. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
j. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
k. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
l. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
m. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
n. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
o. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.
p. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
q. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
r. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
   – manualnego eksportu do pliku w dowolnym momencie czasu,

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

- automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu

s. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
t. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
u. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

Raportowanie

a. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
b. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
c. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
d. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
e. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
f. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
g. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
h. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
i. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

Pozostałe usługi i funkcje

a. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
b. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
c. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
d. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
e. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
f. Urządzenie ma posiadać usługę DNS Proxy.
g. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
h. Urządzenie musi oferować wsparcie dla IEEE 802.10. VLAN.
i. Urządzenie musi mieć zaimplementowane Open API
j. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

Gwarancja i serwis

a. Gwarancja producenta i wsparcie techniczne - nie później niż do 30.06.2026r. na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.

b. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal oraz zdalne administrowanie urządzeniem przez 4 godziny w miesiącu.

Parametry sprzętowe

a. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB.
b. Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy.
c. Liczba portów Ethernet 2,5Gbps - min. 8 z możliwością rozszerzenia do 16.
d. Liczba portów światłowodowych lGbps - min. 2 z możliwością rozszerzenia do 10.
e. Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy:
   - Moduł z 8 interfejsami miedzianymi 2,5Gbps
   - Moduł z 4 interfejsami miedzianymi lOGbps.
   - Moduł z 4 interfejsami światłowodowymi lGbps.
   - Moduł z 8 interfejsami światłowodowymi lGbps.
   - Moduł z 4 interfejsami światłowodowymi lOGbps.
f. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
g. Urządzenie ma być wyposażone w min. 2, różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45.
h. Przepustowość Firewall (1518 bajtów UDP) - minimum lOGbps.
i. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) - minimum 5Gbps.
j. Przepustowość filtrowania Antywirusowego - minimum 1.3 Gbps.
k. Przepustowość tunelu VPN przy szyfrowaniu AES - minimum 2.5Gbps.
l. Maksymalna liczba tuneli VPN IPSec- minimum 1000.
m. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) - minimum 150.
n. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) - minimum 150.
o. Obsługa interfejsów 802.llq (VLAN) - minimum 256.
p. Liczba równoczesnych sesji - minimum 600 000 i nie mniej niż 30 000 nowych sesji/sekundę.
q. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
r. Urządzenie nie ma limitu na liczbę użytkowników.
s. Liczba reguł filtrowania - minimum 16 384.
t. Liczba tras statycznego routingu - minimum 5 120.
u. Liczba tras dynamicznego routingu - minimum 10 000.
v. Możliwość instalacji w szafie RACK 19", wysokość urządzenia 1U.
w. Urządzenie musi być wyposażone w moduł TPM.

CZĘŚĆ 3 Wirtualny serwer do zbierania i przechowywania logów systemowych

Parametry techniczne i funkcjonalne:

a. Implementacja
b. Rozwiązanie jest wspierane co najmniej 4 vCPU oraz 4GB pamięci RAM
c. Rozwiązanie jest wspierane co najmniej 32TB pamięci dyskowej
d. Rozwiązanie obsługuje przechowywanie logów NAT przez 180 dni dla łączy 1G
e. Rozwiązanie obsługuje 30000 EPS dla NAT i 4000 EPS dla Syslog.
f. Rozwiązanie obsługuje następujące hiperwizory, w tym VMware ESXi 5.1/5.5/6.0, VMware Workstation 12 lub nowszy, Linux KVM, Citrix XenServer 7.2.0 lub nowszy

Wydajność
a. Implementacja dostępna w trybie Standalone
b. Implementacja dostępna w trybie Distributed

Monitorowanie urządzeń
a. System umożliwia zbieranie danych z urządzeń Firewall znanych producentów
b. Obsługa stanu użyteczności urządzenia, w tym procesora, pamięci, dysku twardego (w tym pamięci masowej NFS)
c. Statystyki zajętości miejsca na dysku dla różnych typów logów.
d. Trendy odbierania logów oparte na ich typie
e. Trendy odbierania logów oparte na ich źródle pochodzenia
f. Monitor stanu dla urządzeń wysyłających logi
g. Dostosowywalny panel monitora i jego zawartość
h. Obsługa monitorowania stanu dysku twardego i stanu macierzy RAID
i. Możliwość dostosowywania pulpitu nawigacyjnego i obiektów monitora

Log Management
a. Obsługa niestandardowych zapytań lub filtrów dla: dziennika zdarzeń, dziennika sieci, dziennika konfiguracji, dziennika IPS, dziennika zagrożeń, dziennika bezpieczeństwa, dziennika sesji, dziennika PBR, dzienników NAT (w tym NAT444), dziennika URL, dziennika postów BBS, dziennika e-mail, dziennika FTP.
b. Wsparcie dla logów sesji IPv6, logów NAT, logów PBR, logów SLB
c. Obsługa gromadzenia logów i zapytań innych firm
d. Rozróżnianie poziomu logów za pomocą kolorów
e. Wsparcie dla Windows log
f. Obsługa zapytań łączonych według wielu warunków
g. Obsługa wyszukiwania pełno tekstowego w polu adresu URL
h. Obsługa zapytań w tle oraz powiadomień e-mail
i. Możliwość zapamiętywania warunków zapytań
j. Możliwość sprawdzenia stanu zapytania
k. Obsługa zapytań rozproszonych
l. Obsługa dzienników bezpieczeństwa
m. Możliwość analizy, przechowywania i wyświetlania nowych logów zapory sieciowej.
n. Możliwość przesyłania szablonów analizy syslog

Raportowanie
a. Raporty mają możliwość zawierania statystyk takich jak: zasoby systemowe, ranking ilości dzienników urządzeń, ranking zajętości przestrzeni dzienników urządzeń, ranking ilości dzienników, ranking całkowitej przestrzeni dzienników, ranking ilości dzienników na podstawie źródłowego adresu IP, ranking ilości dzienników na podstawie docelowego adresu IP, ranking trendów odbierania dzienników, ilość zagrożeń/ataków, dziennik sesji, dostęp do aplikacji, ranking dostępu do URL itp.
b. Obsługa raportów okresowych: według dnia, tygodnia, miesiąca, kwartału. Raporty mogą być generowane i sortowane według minut, godzin lub dni. Raporty mogą być wysyłane pocztą elektroniczną.
c. Możliwość tworzenia własnych oraz predefiniowane raporty
d. Możliwość raportowania statystyk dotyczących ruchu
e. Eksport raportów jako HTML, PDF oraz WORD

Zarządzanie systemem
a. Możliwość automatycznego czyszczenia dysku w oparciu o zdefiniowane progi

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

b. Dystrybuowanie ustawień w środowiskach rozproszonych
c. Wsparcie dla funkcji NFS
d. Możliwość zdefiniowania zaufanych hostów
e. Obsługa czasu letniego/zimowego
f. Dostęp zarządzający po HTTP oraz HTTPS
g. Możliwość zarządzania hasłami w celu skonfigurowania minimalnej długości i złożoności hasła, maksymalnej liczby niepowodzeń logowania oraz czasu blokady po przekroczeniu maksymalnej liczby niepowodzeń logowania.
h. Możliwość zmiany domyślnej nazwy konta administratora
i. Możliwość użycia platformy HSM w celu centralnego zarządzania
j. Wsparcia dla SSO z poziomu HSM
k. Obsługa zarządzania hasłami, w tym polityka blokowania haseł, polityka haseł
l. Obsługa mechanizmu monitorowania IP i dryfu trasy po nietypowej awarii zasilania
m. Wsparcie weryfikacji dla aktualizacji

Backup logów
a. System wspiera backup poprzez FTP I SFTP
b. Możliwość backupowania logów
c. Możliwość importowania logów
d. Możliwość czyszczenia logów
e. Możliwość przesyłania logów do innych systemów

Warunki licencji
Dostawca zapewni licencję oraz gwarancję na wszystkie dostępne funkcje rozwiązania na okres - nie później niż do 30.06.2026r.

CZĘŚĆ 4 Serwer do systemu zbierania logów krytycznych

parametr	***charakterystyka [wymagania minimalne]***
Obudowa	- Obudowa Rack o wysokości max 2U - min, 16 slotów na dyski 2.5” - Obsługa dysków SSD/SAS/SATA/NVMe - Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. - Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	- Płyta główna z możliwością zainstalowania do dwóch procesorów. - Obsługa procesorów 56 rdzeniowych. - Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. - Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. - Płyta główna powinna obsługiwać do 8TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach

	dwuprocesorowych
Procesor	Zainstalowany jeden procesor min. 16-rdzeniowy, min. 2.0GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku **min. 284** w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	Minimum 128GB DDR5 RDIMM 5600MT/s,

Kontroler RAID	- Sprzętowy kontroler dyskowy, dedykowany dla dysków SSD/SAS/SATA, posiadający
	  - Min. 8GB nieulotnej pamięci cache,
	  - Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
	  - Wsparcie dla dysków samoszyfrujących
	- Sprzętowy kontroler dyskowy, dedykowany dla dysków NVMe, posiadający
	  - Min. 8GB nieulotnej pamięci cache,
	  - Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
	- Wsparcie dla dysków samoszyfrujących

Dyski twarde	- Zainstalowane min.:
	  • 2x dysk SSD SATAU o pojemności min. 1.92TB, Hot-Plug
	  • 4x dysk SSD SATAU o pojemności min. 3.84TB, Hot-Plug
	  • 4x dysk NVMe o pojemności min. 1.92TB, Hot-Plug
	- Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.

Gniazda PCI	min. cztery sloty PCIe
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)

Wbudowane porty	- 4 porty USB w tym min:
	  ○ 1 port USB 3.0,
	  ○ 1 port micro USB
	- min. 2 porty VGA z czego jeden z przodu obudowy
	- możliwość rozbudowy o port RS232

Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	Redundantne, Hot-Plug
Zasilacze	Redundantne, Hot-Plug min. 1100W klasy Titanium
Elementy montażowe	- Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych - Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
System operacyjny/dodatkowe oprogramowanie	Windows Server 2022 Standard wraz z nośnikiem CD/DVD lub inny system serwerowy spełniający poniższe parametry równoważności 35 szt. licencji dostępowych Client Access License do serwerowego systemu operacyjnego. Licencjonowana na użytkownika (User). Licencje wieczyste.
	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.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

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 zapora internetowa (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 dotykiem 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.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

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

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

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 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.

Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

Bezpieczeństwo	- Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. - Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do

	docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. - Możliwość wyłączenia w BIOS funkcji przycisku zasilania. - BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła - Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. - Moduł TPM 2.0 - Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera - Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem - Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); - szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; - możliwość podmontowania zdalnych wirtualnych napędów; - wirtualną konsolę z dostępem do myszy, klawiatury; - wsparcie dla IPv6; - wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; - integracja z Active Directory; - możliwość obsługi przez dwóch administratorów jednocześnie; - wsparcie dla automatycznej rejestracji DNS - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. - możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera - możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera - oraz z możliwością rozszerzenia funkcjonalności o: - Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej - Przesyłanie danych telemetrycznych w czasie rzeczywistym - Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze - Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

- Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
- integracja z Active Directory
- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
- Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
- Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
- Szczegółowy opis wykrytych systemów oraz ich komponentów
- Możliwość eksportu raportu do CSV, HTML, XLS, PDF
- Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.
- Grupowanie urządzeń w oparciu o kryteria użytkownika
- Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
- Szybki podgląd stanu środowiska
- Podsumowanie stanu dla każdego urządzenia
- Szczegółowy status urządzenia/elementu/komponentu
- Generowanie alertów przy zmianie stanu urządzenia.
- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
- Integracja z service desk producenta dostarczonej platformy sprzętowej
- Możliwość przejęcia zdalnego pulpitu
- Możliwość podmontowania wirtualnego napędu
- Kreator umożliwiający dostosowanie akcji dla wybranych alertów
- Możliwość importu plików MIB
- Przesyłanie alertów „as-is” do innych konsol firm trzecich
- Możliwość definiowania ról administratorów
- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
- Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

	- Zdalne uruchamianie diagnostyki serwera. - Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. - Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: - Monitoring: • ilość podłączonych oraz rozłączonych systemów • stan podłączonych urządzeń • informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów • Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia • informacje o statusie gwarancji dla poszczególnych urządzeń • informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń • informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. • Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych • Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. • Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. • Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. • Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. • Monitoring parametrów serwerów z informacją o minimum: o Obciążeniu procesora o Zużyciu pamięci RAM o Temperaturze procesorów o Temperaturze powietrza wlotowego o Zużyciu prądu o Zmianach w fizycznej konfiguracji serwera o Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Monitoring parametrów pamięci masowych z informacją o minimum: o Opóźnieniach o IOPS o Przepustowości o Utylizacji kontrolerów

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

- Pojemność całkowita i dostępna
- Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.
- Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata
- Informacje o poziomie redukcji danych
- Informacje o statusie replikacji oraz snapshotów

- Monitoring parametrów przełączników sieciowych z informacją o minimum:
  - Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny
  - Stanie komponentów: zasilacze, wentylatory
  - Podłączonych hostach
  - Ilości i statusu portów
  - Utylizacji procesora
  - Utylizacji poszczególnych portów
  - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Aktualizacja firmware
  - możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
  - możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
  - możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania
  - możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
  - możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania
- Raporty
  - Możliwość generowania raportów dla serwerów zawierających informację o:
    - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej
    - Średnim obciążeniu: procesorów, pamięci RAM, IO,
  - Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:
    - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji
  - Generowanie raportów do plików CSV i PDF
- Cyberbezpieczeństwo

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

	○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty	- Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 - Serwer musi posiadać deklaracja CE. - Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** - Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja	- Zamawiający wymaga dokumentacji w języku polskim lub angielskim. - Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

użytkownika	warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	- Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres min. 5 lat. - Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. - Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. - Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. - Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. - Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. - Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. - Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. - Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: o Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. o Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. o Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. o Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. o Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

- Wymagane **dołączenie do oferty oświadczenia** potwierdzającego, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
- Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – **dokumenty potwierdzające należy załączyć do oferty.**

CZĘŚĆ 5 Oprogramowanie umożliwiające 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 użytkowanymi przez Zamawiającego systemami teleinformatycznymi wraz z powiadamianiem zespołów bezpieczeństwa.
Zaproponowanie 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,
- Ustawą 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,
- Ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach,
- Ustawą 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, JPX, 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
Interfejs i prezentacja danych	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:

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

	• 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
Raportowanie i alarmowanie licencjonowanie	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.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Zakres prac i wdrożenia	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. 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.

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,

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

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 Posługiwanie 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 –
<u>w zakresie części nr 5:</u>

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

W odniesieniu do pozostałych 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 oceniająca 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

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

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):

CZĘŚĆ 1 –	48730000-4	Pakiety oprogramowania zabezpieczającego
	32420000-3	Urządzenia sieciowe
CZĘŚĆ 2 -	32420000-3	Urządzenia sieciowe
CZĘŚĆ 3 -	48800000-6	Systemy i serwery informacyjne
CZĘŚĆ 4 -	48800000-6	Systemy i serwery informacyjne
CZĘŚĆ 5 -	48730000-4	Pakiety oprogramowania zabezpieczającego

ROZDZIAŁ 4.
TERMIN WYKONANIA ZAMÓWIENIA

Zamówienie będzie wykonane w miejscu siedziby Zamawiającego. Wykonawca wykona zamówienie w terminie:
CZĘŚĆ 1 - **do 60 dni** *[kryterium oceny ofert]* od dnia zawarcia umowy
CZĘŚĆ 2 - **do 60 dni** *[kryterium oceny ofert]* od dnia zawarcia umowy
CZĘŚĆ 3 - **do 60 dni** *[kryterium oceny ofert]* od dnia zawarcia umowy
CZĘŚĆ 4 - **do 60 dni** *[kryterium oceny ofert]* od dnia zawarcia umowy
CZĘŚĆ 5 - **do 60 dni** *[kryterium oceny ofert]* od dnia zawarcia umowy

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.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

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 4 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.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

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 6 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.
3. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z wykonawców, którzy wykonają usługi, do realizacji których te zdolności są wymagane.
4. Zamawiający dopuszcza dowody wykonania usług, o których mowa powyżej z ceną wyrażoną w innej walucie niż PLN, mieszczącej się w tabeli Narodowego Banku Polskiego (NBP).
5. W takim przypadku Zamawiający przeliczy cenę każdej oferty wyrażoną w walucie innej niż polska stosując średni kurs NBP z dnia zamieszczenia ogłoszenia o zamówieniu do Biuletynu Zamówień Publicznych.
6. Jeżeli w dniu publikacji ogłoszenia o zamówieniu w Biuletynie Zamówień Publicznych, Narodowy Bank Polski nie publikuje średniego kursu danej waluty, za podstawę przeliczenia przyjmuje się średni kurs

waluty publikowany pierwszego dnia, po dniu publikacji ogłoszenia o zamówieniu w Biuletynie Zamówień Publicznych, w którym zostanie on opublikowany.

7. Zamawiający, w stosunku do Wykonawców wspólnie ubiegających się o udzielenie zamówienia, w odniesieniu do warunku dotyczącego zdolności technicznej lub zawodowej – dopuszcza łączne spełnianie warunku przez Wykonawców.
8. Zamawiający może na każdym etapie postępowania, uznać, że wykonawca nie posiada wymaganych zdolności, jeżeli posiadanie przez wykonawcę sprzecznych interesów, w szczególności zaangażowanie zasobów technicznych lub zawodowych wykonawcy w inne przedsięwzięcia gospodarcze wykonawcy może mieć negatywny wpływ na realizację zamówienia.
9. 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.

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 zakłócenie 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 zakłócenia 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 zakłócenie 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 postepowania. 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

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

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 oraz spełnia warunki udziału w postępowaniu.
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 oraz spełnia warunki udziału w postępowaniu.
4. W przypadku wspólnego ubiegania się o zamówienie przez wykonawców, oświadczenie, o którym mowa w ust. 1, składa każdy z Wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu lub kryteriów selekcji w zakresie, w jakim każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu lub kryteriów selekcji.
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 oraz odpowiednio spełnianie warunków udziału w postępowaniu lub kryteriów selekcji, w zakresie, w jakim Wykonawca powołuje się na jego zasoby.
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. <u>Na wezwanie Zamawiającego Wykonawca zobowiązany jest do złożenia następujących oświadczeń lub dokumentów potwierdzających brak podstaw wykluczenia:</u>
   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 5 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 5 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. I 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. l, 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 poświadczonej 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 zgody 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 przesłanki 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. Osobą uprawnioną do kontaktu z Wykonawcami jest:
1.1. W zakresie proceduralnym: Adriana Tarakan, tel. 58 588 43 81 wew. 44;
1.2. W zakresie merytorycznym: Adam Gilla, tel. 58 588 43 81 wew. 15
2. Komunikacja w postępowaniu o udzielenie zamówienia, w tym składanie ofert, wymiana informacji oraz przekazywanie dokumentów lub oświadczeń między zamawiającym a wykonawcą, z uwzględnieniem wyjątków określonych w ustawie Pzp, odbywać się przy użyciu środków komunikacji elektronicznej. Przez środki komunikacji elektronicznej rozumie się środki komunikacji elektronicznej zdefiniowane w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.
3. Postępowanie prowadzone jest w języku polskim w formie elektronicznej za pośrednictwem platformazakupowa.pl pod adresem: https://platformazakupowa.pl/pn/zblewo
4. Korzystanie z platformy zakupowej przez wykonawcę jest bezpłatne.
5. W celu skrócenia czasu udzielenia odpowiedzi na pytania preferuje się, aby komunikacja między zamawiającym a wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje,

przekazywane były w formie elektronicznej za pośrednictwem platformazakupowa.pl i formularza „Wyślij wiadomość do zamawiającego". Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem platformazakupowa.pl poprzez kliknięcie przycisku „Wyślij wiadomość do zamawiającego" po których pojawi się komunikat, że wiadomość została wysłana do zamawiającego.

6. W sytuacjach awaryjnych z wyjątkiem składania ofert zamawiający dopuszcza komunikację elektroniczną poprzez email: zamowieniapubliczne@zblewo.pl lub gmina@zblewo.pl.
7. Zamawiający będzie przekazywał wykonawcom informacje w formie elektronicznej za pośrednictwem platformazakupowa.pl. Informacje dotyczące odpowiedzi na pytania, zmiany specyfikacji, zmiany terminu składania i otwarcia ofert zamawiający będzie zamieszczał na platformie w sekcji „Komunikaty". Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny wykonawca, będzie przekazywana w formie elektronicznej za pośrednictwem platformazakupowa.pl do konkretnego wykonawcy.
8. Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na platformazakupowa.pl przesłanych przez zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.
9. Zamawiający, zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 30 grudnia 2020r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020r. poz. 2452), określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na platformazakupowa.pl, tj.:

9.1. stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
9.2. komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje,
9.3. zainstalowana dowolna przeglądarka internetowa, w przypadku Internet Explorer minimalnie wersja 10 0.,
9.4. włączona obsługa JavaScript,
9.5. zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,
9.6. platformazakupowa.pl działa według standardu przyjętego w komunikacji sieciowej - kodowanie UTF8,
9.7. oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.

10. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:

10.1. akceptuje warunki korzystania z platformazakupowa.pl określone w Regulaminie zamieszczonym na stronie internetowej pod linkiem w zakładce „Regulamin" oraz uznaje go za wiążący,
10.2. zapoznał i stosuje się do Instrukcji składania ofert/wniosków dostępnej pod linkiem: https://drive.google.eom/file/d/1Kd1DttbBeiNWt4q4slS4t76IZVKPbkyD/view

11. Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania z platformazakupowa.pl, w szczególności za sytuację, gdy zamawiający zapozna się z treścią oferty przed upływem terminu składania ofert (np. złożenie oferty w zakładce „Wyślij wiadomość do zamawiającego"). Taka oferta zostanie uznana przez Zamawiającego za ofertę handlową i nie będzie brana pod uwagę w przedmiotowym postępowaniu ponieważ nie został spełniony obowiązek narzucony w art. 221 ustawy Pzp.
12. Zamawiający informuje, że instrukcje korzystania z platformazakupowa.pl dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu platformazakupowa.pl znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje

13. W korespondencji kierowanej do Zamawiającego Wykonawcy powinni posługiwać się numerem przedmiotowego postępowania.
14. Wykonawca może zwrócić się do zamawiającego z wnioskiem o wyjaśnienie treści SWZ.
15. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem że wniosek o wyjaśnienie treści SWZ wpłynął do zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert.
16. Jeżeli zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w pkt 7.15 SWZ, przedłuża termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia ofert, W przypadku gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie, o którym mowa w pkt 7.15 SWZ, zamawiający nie ma obowiązku udzielania wyjaśnień SWZ oraz obowiązku przedłużenia terminu składania ofert.
17. Przedłużenie terminu składania ofert, o których mowa w pkt 7.16 SWZ, nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.
18. Treść zapytań wraz z wyjaśnieniami zamawiający udostępnia, bez ujawniania źródła zapytania, na stronie internetowej prowadzonego postępowania: https://platformazakupowa.pl/pn/zblewo, w zakładce „Komunikaty publiczne".

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

Wykonawca może złożyć ofertę na jedną lub więcej części. Ocenie będzie podlegać oddzielnie każda część zamówienia. Wykonawca może złożyć tylko jedną ofertę na każdą część zamówienia.
Oferta winna być:

1. sporządzona na podstawie załączników niniejszej SWZ w języku polskim,
2. złożona przy użyciu środków komunikacji elektronicznej tzn. za pośrednictwem platformazakupowa.pl,
3. podpisana kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione.
7. Podpisy kwalifikowane wykorzystywane przez wykonawców do podpisywania wszelkich plików muszą spełniać „Rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku".

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

8. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny. Zamawiający wymaga dołączenia odpowiedniej ilości plików tj. podpisywanych plików z danymi oraz plików podpisu w formacie XAdES.
9. Zgodnie z art. 18 ust. 3 ustawy Pzp, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Jeżeli wykonawca, nie później niż w terminie składania ofert, w sposób niebudzący wątpliwości zastrzegł, że nie mogą być one udostępniane oraz wykazał, załączając stosowne wyjaśnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Na platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.
10. Wykonawca, za pośrednictwem platformazakupowa.pl może przed upływem terminu do składania ofert zmienić lub wycofać ofertę. Sposób dokonywania zmiany lub wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje.
11. Dokumenty i oświadczenia składane przez wykonawcę powinny być w języku polskim. W przypadku załączenia dokumentów sporządzonych w innym języku niż dopuszczony, wykonawca zobowiązany jest załączyć tłumaczenie na język polski.
12. Zgodnie z definicją dokumentu elektronicznego z art. 3 ust. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, opatrzenie pliku zawierającego skompresowane dane kwalifikowanym podpisem elektronicznym jest jednoznaczne z podpisaniem oryginału dokumentu, z wyjątkiem kopii poświadczonych odpowiednio przez innego wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia, przez podmiot, na którego zdolnościach lub sytuacji polega wykonawca, albo przez podwykonawcę.
13. Na podstawie §8 Rozporządzenia Prezesa Rady Ministrów z dnia 30.12.2020r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie, w przypadku przekazywania w postępowaniu dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku odpowiednio kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. Zamawiający zaleca jednak w przypadku gdy wykonawca pakuje dokumenty np. w plik o rozszerzeniu .zip - wcześniejsze podpisanie każdego ze skompresowanych plików.
14. Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty wynosi 150 MB natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.

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;

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

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.

Zalecenia (rekomendacje) zamawiającego.

1. Rozszerzenia plików wykorzystywanych przez Wykonawców powinny być zgodne z załącznikiem nr 2 do „Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych", zwanego dalej Rozporządzeniem KRI.
2. Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .docx .xls .xlsx .jpg (.jpeg) ze szczególnym wskazaniem na .pdf
3. W celu ewentualnej kompresji danych zamawiający rekomenduje wykorzystanie jednego z rozszerzeń:
   28.3.1. .zip
   28.3.2. .7Z
4. Wśród rozszerzeń powszechnych a niewystępujących w rozporządzeniu KRI występują: .rar .gif .bmp .numbers .pages. Dokumenty złożone w takich plikach zostaną uznane za złożone nieskutecznie.
5. Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi maksymalnie 10MB, oraz na ograniczenie wielkości plików podpisywanych w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi maksymalnie 5MB.
6. W przypadku stosowania przez wykonawcę kwalifikowanego podpisu elektronicznego:

6.1. ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu, zamawiający zaleca, w miarę możliwości, przekonwertowanie plików składających się na ofertę na rozszerzenie .pdf i opatrzenie ich podpisem kwalifikowanym w formacie PAdES.

6.2. pliki w innych formatach niż pdf zaleca się opatrzyć podpisem w formacie XAdES o typie zewnętrznym. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.

6.3. Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.

7. Zamawiający zaleca aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju. Podpisywanie różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików.
8. Zamawiający zaleca, aby wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.
9. Osobą składającą ofertę powinna być osoba kontaktowa podawana w dokumentacji.
10. Ofertę należy przygotować z należytą starannością dla podmiotu ubiegającego się o udzielenie zamówienia publicznego i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert. Sugerujemy złożenie oferty na 24 godziny przed terminem składania ofert.
11. Jeśli wykonawca pakuje dokumenty np. w plik o rozszerzeniu .zip zaleca się wcześniejsze podpisanie każdego ze skompresowanych plików.
12. Zamawiający zaleca aby nie wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich podpisem kwalifikowanym. Może to skutkować naruszeniem integralności plików co równoważne będzie z koniecznością odrzucenia oferty.

ROZDZIAŁ 13.
WADIUM

1. Zamawiający nie wymaga wniesienia wadium.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

ROZDZIAŁ 14.
TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca będzie związany złożoną ofertą przez 30 dni, tj. do dnia **28.12.2024 r.**
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 wraz z wymaganymi dokumentami należy umieścić na platformazakupowa.pl pod adresem: https://platformazakupowa.pl/pn/zblewo **do dnia 29.11.2024 r 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 **29.11.2024 r., o godz. 10:05.** 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 udzielnie 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 wszystkich części zamówienia:

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

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

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 dostawy

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, w tym w szczególności z zabezpieczeniem należytego wykonania umowy.
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) wniesienia zabezpieczenia należytego wykonania umowy,
   b) 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.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

ROZDZIAŁ 19.
PROJEKTOWANE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI TEJ UMOWY

1. Jako odrębny Załącznik nr 6 do SWZ Zamawiający zamieścił 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 przysługuje 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.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

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 i o spełnianiu warunków udziału w postępowaniu: **Załącznik nr 2;**
3. Oświadczenie dotyczące przynależności lub braku przynależności do tej samej grupy kapitałowej: **Załącznik nr 3;**
4. Wzór Umowy: **Załącznik nr 6;**
5. Oświadczenie wykonawców wspólnie ubiegających się o udzielenie zamówienia – **załącznik nr 4;**
6. Oświadczenie Wykonawcy – **Załącznik nr 5**
7. Wymagania dotyczące próbki przedmiotu zamówienia oraz zasady i zakres jej badania – **Załącznik nr 7.**

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Załącznik nr 1 do SWZ

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 pn. **Dostawa sprzętu i oprogramowania wraz z usługą wdrożenia realizowana w ramach projektu grantowego „Cyberbezpieczny Samorząd”** – *nr ref.:* **RO.271.30.2024**

1. Oferujemy wykonanie przedmiotu zamówienia **za ryczałtową cenę:**

CZĘŚĆ ZAMÓWIENIA	Opis	Model / Producent	Ilość	Cena jednostkowa netto [PLN]	Wartość netto [PLN]	Podatek Vat [%]	Wartość brutto [PLN]
CZĘŚĆ 1	System NDR (Network Detection and Response)		1				
CZĘŚĆ 2	Rozbudowa zabezpieczeń logicznych (firewall) – zakup UTM		1				
CZĘŚĆ 3	Wirtualny serwer do zbierania i przechowywania logów systemowych		1				
CZĘŚĆ 4	Serwer do systemu zbierania logów krytycznych		1				
CZĘŚĆ 5	Oprogramowanie umożliwiające monitoring usług i użytkowanych systemów		1				

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

Skrócenie terminu realizacji	
0 dni	☐
30 dni	☐

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, że[1]:
   - ☐ 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 jesteśmy[2]:
   - ☐ 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 RODO[4] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

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)

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Załącznik nr 2 do SWZ

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 ORAZ SPEŁNIANIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU
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:

I. Spełnianie warunków udziału w postępowaniu

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez zamawiającego w SWZ oraz ogłoszeniu o zamówieniu.

II. Przesłanek 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*

Załącznik nr 3 do SWZ

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.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Załącznik nr 4 do SWZ

[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, <u>oświadczam, że:</u>**

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.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Załącznik nr 5 do SWZ

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

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Załącznik nr 6 do SWZ

UMOWA NR ..... [wzór]

zawarta w dniu ..... 2024 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. „Dostawa sprzętu i oprogramowania wraz z usługą wdrożenia realizowana w ramach projektu grantowego „Cyberbezpieczny Samorząd".**
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:
   CZĘŚĆ 1 System NDR (Network Detection and Response)
   CZĘŚĆ 2 Rozbudowa zabezpieczeń logicznych (firewall) – zakup UTM
   CZĘŚĆ 3 Wirtualny serwer do zbierania i przechowywania logów systemowych
   CZĘŚĆ 4 Serwer do systemu zbierania logów krytycznych
   CZĘŚĆ 5 Oprogramowanie umożliwiające monitoring usług i użytkowanych systemów

   (pozostawić właściwe części)

§ 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.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

§ 3

WYNAGRODZENIE

1. Wynagrodzenie z tytułu wykonania przedmiotu umowy będzie stanowiła kwota ..... **zł brutto** (słownie: .....), ...zł netto (słownie:.....), podatek VAT....%, 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 niezmienne 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, 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”:

   ZAMAWIAJĄCY/NABYWCA PŁATNIK/ODBIORCA

   .....

   .....

   .....

   NIP .....
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.
10. Zgodnie z ustawą z dnia 9 listopada 2018r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prawnym (tj. Dz.U. z 2020 r. poz.

1666 z późn. zm.) istnieje możliwość wystawiania i przekazania Zamawiającemu faktury VAT drogą elektroniczną za pośrednictwem Platformy Elektronicznego Fakturowania https://brokerperfexpert.efaktura.gov.pl, NIP: .....

§ 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 jakiekolwiek 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:

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

– · 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, o którym mowa w § 8 ust. 7 umowy;
   3) 0,25% wynagrodzenia umownego brutto, określonego w § 4 ust. 1 umowy, za każdą godzinę zwłoki w realizacji zobowiązań wynikających z § 13 ust. 4 lit. a) i b) umowy;
   4) 0,25% wynagrodzenia umownego brutto, określonego w § 4 ust. 1 umowy, za każdy dzień zwłoki w realizacji zobowiązań wynikających z § 13 ust. 4 lit. c) umowy;
   5) 0,25% wynagrodzenia umownego brutto, określonego w § 4 ust. 1 umowy, za każdą godzinę zwłoki w realizacji zobowiązań wynikających z § 13 ust. 3 lit. a) i b) 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 przesłanki 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 potracenia 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 upłynie 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 ciążą 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 opóźnienia w wykonywaniu swoich zobowiązań umownych, powstałego na skutek działania siły wyższej,
      – okoliczności leżących po stronie Zamawiającego i nie wynikających z przyczyn leżących po stronie

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

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.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

§ 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 wymogi określone w SWZ, Opisie przedmiotu zamówienia oraz niniejszej umowie.
2. Wykonawca udziela gwarancji na dostarczane w ramach umowy oprogramowanie na okres nie później niż do 30.06.2026r. zgodnie z specyfikacją warunków zamówienia.
3. Okres gwarancji wskazany w ust. 2 liczy się od daty podpisania przez obie strony protokołu odbioru końcowego przedmiotu umowy.
4. Okres gwarancji ulega wydłużeniu o czas liczony od zawiadomienia Wykonawcy o wystąpieniu wady/usterki do momentu jej usunięcia.
5. Odpowiedzialność z tytułu gwarancji obejmuje zarówno wady/usterki powstałe z przyczyn tkwiących w przedmiocie umowy w chwili dokonania jego odbioru przez Zamawiającego.
6. 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) poprawność uruchomionych i wdrożonych mechanizmów integracji i wymiany danych pomiędzy wdrożonym rozwiązaniem a istniejącymi rozwiązaniami Zamawiającego
   e) zgodność wdrożonego rozwiązania z właściwymi przepisami prawa na dzień podpisania protokołu odbioru.
   f) zapewnienie prawidłowego działania przedmiotu umowy w okresie gwarancji,
7. 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.
8. Wszelkie świadczenia Wykonawcy w okresie gwarancji są bezpłatne i nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów.
9. Okres rękojmi jest równy okresowi gwarancji.
10. 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.
11. 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.
12. 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. Licencje, o których mowa w ust. 1 muszą być licencjami udzielonymi na czas określony w specyfikacji

warunków zamówienia.

3. Wykonawca nie będzie uprawniony do wypowiedzenia Licencji, o ile zamawiający nie naruszy jej postanowień.
4. Wykonawca przekazuje niewyłączne licencje, na inne dostarczone komponenty, które są niezbędne do prawidłowego działania systemu.
5. 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, wydzierżawiania, udzielania dalszych sublicencji lub innego przenoszenia swych praw na osoby trzecie.
6. 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.
7. Licencje uprawniają do korzystania z utworów co najmniej na terytorium Rzeczypospolitej Polskiej.
8. 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.
9. Udzielnie Licencji na warunkach określonych w niniejszym paragrafie zostanie potwierdzone stosownym dokumentem licencyjnym (certyfikatem), podpisanym przez osobę(y) uprawnione do jej udzielenia.

§ 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 spełniania 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:**

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Załącznik nr 7 do SWZ
Wymagania dotyczące próbki przedmiotu zamówienia oraz zasady i zakres jej badania
Dot. CZĘŚCI 5

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 próbki 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

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

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 systemów użytkowanych przez Zamawiającego wraz z możliwością wysyłania powiadomień e-mail/sms

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 komunikacje jest wyłączona) b. zalogować się w systemie obsługującym komunikacje 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 zimna statusu informująca o prawidłowym działaniu) d. zalogować się w systemie obsługującym komunikacje 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 komunikacje z systemem i wysłać testową wiadomość h. zweryfikować powstanie komunikatu błędu w systemie monitorującym i. usunąć sabotaż

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

	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.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl