OPIS PRZEDMIOTU ZAMÓWIENIA

Kody i nazwy opisujące przedmiot zamówienia (CPV):
48000000-8 Pakiety oprogramowania i systemy informatyczne
32424000-1 Infrastruktura sieciowa
722680001 Usługi dostawy oprogramowania
722650000 Usługi konfiguracji oprogramowania
722630006 Usługi wdrażania oprogramowania
31122000-7 Jednostki prądotwórcze
31682530-4 Awaryjne urządzenia energetyczne

Przedmiotem zamówienia jest zakup i wdrożenie oprogramowania oraz zakup agregatu prądotwórczego w ramach projektu grantowego pn. „Cyberbezpieczny Samorząd" dofinansowanego w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Działania 2.2 pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa", zgodnie z Regulaminem Konkursu Grantowego „Cyberbezpieczny Samorząd":

Część I: Zakup i dostawa licencji, wdrożenie, konfiguracja, uruchomienie oraz przekazanie do użytkowania oprogramowania oraz usług służących podniesieniu poziomu cyberbezpieczeństwa, w szczególności:

1. Oprogramowanie do ochrony danych osobowych (DLP) ,
2. System kontroli dostępu do sieci komputerowej (NAC),
3. System monitorowania i ochrony cyberbezpieczeństwa (SIEM),
4. Wdrożenie, konfiguracja i migracja do środowiska chmurowego Microsoft 365.

Część II: Zakup agregatu prądotwórczego.

CZĘŚĆ I

1. Parametry dla DLP:

1.1. Klasyfikacja danych, kontrola przepływu informacji (USB, e-mail, chmura), audyt bezpieczeństwa, a także zarządzanie drukowaniem i ochrona urządzeń przenośnych,

1.2. Monitorowanie aktywności użytkowników (Insight): Audyt czasu pracy, kontrola używanych aplikacji i odwiedzanych stron WWW, co pozwala wykryć podejrzane działania.

1.3. Zarządzanie urządzeniami i drukiem: Kontrola nad nośnikami zewnętrznymi (USB) oraz możliwość audytu i limitowania drukowania (kolor/duplex).

1.4. Ochrona w chmurze i BYOD: Zabezpieczenie danych na urządzeniach służbowych i prywatnych (Bring Your Own Device) używanych w pracy.

1.5. Zgodność z przepisami (Compliance): Automatyczne raportowanie i audyt ułatwiające zachowanie zgodności z RODO, ISO 27001, HIPAA i innymi standardami.

1.6. Obsługa systemów operacyjnych : Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi, Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi, MacOS 12 lub nowszy

1.7. Konsola administracyjna i komunikaty klienta w języku polskim.

1.8. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta,

1.9. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.

1.10. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.

1.11. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.

1.12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania,

1.13. Administrator musi mieć możliwość aby tworzyć, usuwać konta administratorów w konsoli programu.

1.14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).

1.15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.

1.16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.

1.17. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.

1.18. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.

1.19. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.

1.20. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.

1.21. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.

1.22. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.

1.23. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.

1.24. Licencja bezterminowa (perpetual license), zapewniająca Zamawiającemu nieograniczone czasowo prawo do użytkowania wszystkich dostarczonych komponentów systemu dla 150 użytkowników z rocznym serwisem,

1.25. Licencja bezterminowa musi obejmować wszystkie funkcjonalności wymagane w niniejszym OPZ, bez konieczności ponoszenia dodatkowych opłat abonamentowych warunkujących dalsze korzystanie z systemu.

1.26. Licencja musi umożliwiać instalację i eksploatację rozwiązania w infrastrukturze teleinformatycznej Zamawiającego bez obowiązku korzystania z usług chmurowych producenta.

1.27. Zamawiający wymaga, aby licencjonowanie nie było uzależnione od wolumenu przechowywanych logów, liczby analizowanych zdarzeń lub ilości danych retencjonowanych w systemie.

1.28. System musi umożliwiać obsługę co najmniej 300 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia, w tym użytkowników gościnnych, chyba że Zamawiający wskaże inną liczbę przed ogłoszeniem postępowania,

1.29. System musi umożliwiać dalszą rozbudowę licencyjną w przypadku wzrostu liczby

obsługiwanych urządzeń lub użytkowników,

1.30. Wykonawca zapewni co najmniej 12 miesięcy wsparcia producenta lub równoważnego wsparcia technicznego dla dostarczonego rozwiązania,

1.31. W przypadku zakończenia okresu wsparcia technicznego Zamawiający zachowuje pełną możliwość dalszego użytkowania wdrożonego systemu wraz z wszystkimi skonfigurowanymi funkcjonalnościami.

2. Parametry dla NAC:

2.1. System ma służyć do aktywnego zapobiegania dostępowi do sieci komputerowej przez nieautoryzowanych użytkowników i nieautoryzowane urządzenia końcowe. System powinien umożliwiać identyfikację, uwierzytelnianie, autoryzację, profilowanie, monitorowanie i egzekwowanie polityk dostępu w sieci przewodowej, bezprzewodowej oraz w obszarze dostępu gościnnego,

2.2. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.

2.3. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)

2.4. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.

2.5. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.

2.6. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.

2.7. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.

2.8. System musi umożliwiać obsługę co najmniej 300 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 10 000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.

2.9. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.

2.10. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.

2.11. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym: VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x,

2.12. Maszyny fizyczne - serwery wspierane przez producenta,

2.13. System musi posiadać funkcjonalność serwerów:

a) RADIUS dla infrastruktury sieciowej,

b) OTP dla infrastruktury VPN, Captive Portal, Tacacs+,

c) SYSLOG,

d) TACACS+,

e) Monitoringu,

f) DHCP,

g) polityk uwierzytelniania i kontroli dostępu 802.1X,

h) WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.

2.14. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.

2.15. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.

2.16. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.

2.17. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now.

2.18. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.

2.19. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.

2.20. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.

2.21. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.

2.22. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.

2.23. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).

2.24. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.

2.25. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).

2.26. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.

2.27. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.

2.28. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.

2.29. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.

2.30. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.

2.31. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.

2.32. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.

2.33. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.

2.34. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.

2.35. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.

2.36. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.

2.37. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.

2.38. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).

2.39. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.

2.40. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.

2.41. System musi posiadać funkcję personalizacji strony gościnnej.

2.42. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.

2.43. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.

2.44. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.

2.45. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.

2.46. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.

2.47. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.

2.48. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.

2.49. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).

2.50. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.

2.51. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.

2.52. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.

2.53. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.

2.54. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.

2.55. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.

2.56. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.

2.57. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.

2.58. System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.

2.59. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).

2.60. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.

2.61. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:

a) Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności,

b) Czy włączony jest firewall,

c) Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur,

d) Czy jest włączone szyfrowanie dysku systemowego,

e) Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory,

f) Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora,

g) Czy w systemie są uruchomione procesy wskazane przez administratora,

h) Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności,

i) Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem wartości klucza rejestru i typu wartości: Number, String, Version

2.62. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.

2.63. System musi współpracować z serwerem tokenów.

2.64. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:

a) Microsoft Windows,

b) Mac OS,

c) iOS,

d) Android

2.65. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).

2.66. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

2.67. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.

2.68. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:

a) MAC,

b) PAP/ASCII,

c) CHAP,

d) SNMP,

e) 802.1X.

2.69. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.

2.70. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.

2.71. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).

2.72. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:

a) Tożsamość/Urządzenie końcowe,

b) Grupa tożsamości/urządzeń końcowych,

c) Parametry urządzeń końcowych, min: system operacyjny, wersja,

d) Atrybuty Active Directory,

e) Jednostka organizacyjna tożsamości/urządzeń końcowych,

f) Urządzenia sieciowe sieci przewodowej, bezprzewodowej,

g) Grupy urządzeń sieciowych,

h) Porty urządzeń sieciowych,

i) Grupy portów urządzeń sieciowych,

j) Jednostka organizacyjna portów,

k) Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),

l) Data, czas ważności polityki,

m) Wewnętrzny Captive Portal,

n) Metoda autoryzacji.

2.73. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.

2.74. System musi wspierać funkcjonalność IP-to-ID Mapping, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.

2.75. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości,

urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.

2.76. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.

2.77. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.

2.78. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.

2.79. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.

2.80. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.

2.81. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.

2.82. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.

2.83. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.

2.84. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.

2.85. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

2.86. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.

2.87. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:

a) możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.

b) możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.

2.88. Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).

2.89. System musi posiadać funkcję zintegrowanego serwera DHCP.

2.90. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.

2.91. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:

a) Uruchamianie usługi dla wybranych podsieci,

b) Przypisanie ustalonego adresu IP dla adresu MAC.

c) Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,

d) Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,

e) Możliwość określania braku dostępu dla wybranych adresów MAC,

f) Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,

g) Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,

h) Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,

i) Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,

j) Dokonywanie zmian bez konieczności wyłączania usług.

2.92. W zakresie obsługi serwerów TACACS+ System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:

a) grupowanie urządzeń końcowych oraz administratorów,

b) tworzenia haseł administratorom,

c) tworzenie listy komend uprawnień dla administratorów,

d) raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.

e) umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.

f) umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.

g) wspierać logowanie administratorów za pomocą tokenów OTP.

h) umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

2.93. System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

a) Monitoring autoryzacji,

b) Monitoring dla zdarzeń systemowych,

c) Monitoring dla zdarzeń DHCP,

d) Monitoring dla tożsamości,

e) Monitoring dla urządzeń końcowych,

f) Monitoring dla urządzeń sieciowych,

g) Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email,

h) Raport ze zdarzeń logowania z informacją o nadam adresie IP,

i) Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług,

j) Raport z logów DHCP z informacją o polityce dostępu logowania do sieci,

k) Posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym,

l) Wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie,

m) Wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku,

n) Wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych,

o) Posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja,

p) Umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi,

q) Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.

r) Raport zdarzeń Microsoft Active Directory, minimum:

- Logowania, wylogowania z system w tym błędne logowania,
- Logowania do sieci 802.1X,

2.94. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:

a) wiadomości e-mail,

b) Syslog,

c) notyfikacji systemowych.

2.95. Alarmy mogą być generowane w sytuacjach, min:

a) Ilości obsługiwanych transakcji RADIUS,

b) Opóźnienie obsługi transkacji RADIUS,

c) Statusu krytycznego modułów,

2.96. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:

a) badanie łączności IP za pomocą ping, traceroute,

b) tcpdump protokołów RADIUS, TACACS+,

c) wyszukiwanie zdarzeń RADIUS z uwzględnieniem:

- nazwy użytkownika,
- adresu MAC,
- statusu uwierzytelnienia (udana lub nieudana),
- powodu, jeżeli uwierzytelnienie nieudane,
- zakresu czasowego, co do dnia, godziny i minuty,

d) wykonanie zdalnego polecenia na urządzeniu sieciowym

2.97. Wymagania dotyczące wdrożenia:

a) dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta.

b) Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA).

c) Konfiguracja urządzenia firewall (dodatnie VLAN-u gościnnego, ustawienie polityk, etc.).

d) Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).

e) Integracja dostarczanych urządzeń sieciowych (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach.

f) Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy.

g) Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.

h) Przeprowadzenie szkolenia dla administratorów z konfiguracji i administrowania Systemem NAC. Dwudniowe szkolenie online zdalne dla do 4 osób po 6h dziennie.

i) Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni po zakończeniu wdrożenia.

2.98. Wykonawca zapewni 2-dniowe warsztaty (2 dni x 6h) w zakresie użytkowania i administrowania wdrożonym systemem NAC. Warsztaty zostaną przeprowadzone dla maksymalnie 4 osób i będą uwzględniać informacje z zakresu wdrożonego systemu NAC. Po zakończeniu warsztatów, uczestnicy otrzymają zaświadczenia potwierdzające uczestnictwo w szkoleniach/warsztatach oraz nabycie umiejętności obsługi systemu NAC. Warsztaty odbędą się w formie zdalnej. Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej. Szczegółowy plan, zakres i terminy szkoleń/warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym.

2.99. Wykonawca dostarczy wraz dożywotnią licencją systemu NAC – 12 miesięczną licencje na wsparcie producenta oprogramowania. Licencja ta powinna obejmować minimum:

a) Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC,

b) Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia,

c) Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów,

d) Dostęp do dokumentacji i instrukcji na stronie internetowej,

e) Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

2.100. Oferowane rozwiązanie musi być dostarczone w modelu licencji bezterminowej (perpetual license), zapewniającej Zamawiającemu nieograniczone czasowo prawo do użytkowania wszystkich dostarczonych komponentów systemu.

2.101. Licencja bezterminowa musi obejmować wszystkie funkcjonalności wymagane w niniejszym OPZ, bez konieczności ponoszenia dodatkowych opłat abonamentowych warunkujących dalsze korzystanie z systemu.

2.102. W przypadku zakończenia okresu wsparcia technicznego Zamawiający zachowuje pełną możliwość dalszego użytkowania wdrożonego systemu wraz z wszystkimi skonfigurowanymi funkcjonalnościami.

2.103. Licencja musi umożliwiać instalację i eksploatację rozwiązania w infrastrukturze teleinformatycznej Zamawiającego bez obowiązku korzystania z usług chmurowych producenta.

2.104. Zamawiający wymaga, aby licencjonowanie nie było uzależnione od wolumenu przechowywanych logów, liczby analizowanych zdarzeń lub ilości danych retencjonowanych

w systemie.

3. Parametry SIEM:

3.1. Rozwiązanie ma zapewnić centralne gromadzenie, analizę, korelację i wizualizację zdarzeń bezpieczeństwa pochodzących z infrastruktury informatycznej Zamawiającego oraz wspierać realizację wymagań wynikających z ustawy o krajowym systemie cyberbezpieczeństwa, Dyrektywy NIS2, Krajowych Ram Interoperacyjności,, normy ISO/IEC 27001, RODO,

3.2. System musi umożliwiać integrację z :

a) Active Directory,
b) Microsoft Entra ID,
c) Microsoft 365,
d) VMware,
e) Hyper-V,
f) systemami firewall,
g) systemami EDR,
h) platformami Threat Intelligence,
i) systemami Service Desk.

3.3. Integracja musi być realizowana przez :

a) API REST,
b) Syslog,
c) webhooki,
d) konektory producenta.

3.4. System musi umożliwiać:

a) Zbieranie logów z systemów Windows Server,
b) zbieranie logów z systemów Linux,
c) zbieranie logów z urządzeń sieciowych,
d) zbieranie logów z zapór sieciowych,
e) zbieranie logów z systemów antywirusowych i EDR,
f) zbieranie logów z baz danych,
g) zbieranie logów z aplikacji biznesowych,
h) zbieranie logów z usług chmurowych.

3.5. System musi obsługiwać :

a) Syslog,
b) Windows Event Forwarding,
c) API REST,
d) SNMP,
e) agentów instalowanych na stacjach i serwerach.

3.6. System musi umożliwiać:

a) analizę zdarzeń w czasie rzeczywistym,

b) tworzenie reguł korelacyjnych,

c) wieloetapową korelację zdarzeń,

d) identyfikację ataków prowadzonych w wielu etapach,

e) identyfikację nietypowych zachowań użytkowników i systemów poprzez analizę zdarzeń bezpieczeństwa i mechanizmy detekcyjne.

3.7. System powinien posiadać gotowe reguły odnoszące się do :

a) MITRE ATT&CK,

b) OWASP Top 10,

c) CIS Controls.

3.8. Rozwiązanie musi zapewniać:

a) wykrywanie prób nieautoryzowanego dostępu,

b) wykrywanie eskalacji uprawnień,

c) wykrywanie ransomware,

d) wykrywanie malware,

e) wykrywanie wykorzystania znanych podatności,

f) wykrywanie komunikacji z adresami znajdującymi się na listach IOC

3.9. System musi umożliwiać

a) monitorowanie zmian plików,

b) monitorowanie zmian katalogów,

c) monitorowanie zmian rejestru systemów Windows,

d) monitorowanie zmian konfiguracji systemów operacyjnych,

e) określanie wyjątków monitorowania.

3.10. Alert musi zawierać:

a) datę zmiany,

b) użytkownika dokonującego zmiany,

c) zakres zmiany,

d) nazwę zasobu.

3.11. System musi :

a) automatycznie identyfikować podatności bezpieczeństwa,

b) wykorzystywać bazę CVE,

c) przypisywać ocenę ryzyka CVSS,

d) prezentować listę podatności według krytyczności,

e) umożliwiać tworzenie raportów podatności.

3.12. Rozwiązanie musi umożliwiać :

a) ocenę zgodności konfiguracji z benchmarkami bezpieczeństwa,

b) automatyczne wykrywanie odstępstw od polityk bezpieczeństwa,

c) raportowanie poziomu zgodności.

3.13. Wymagane benchmarki:
   a) CIS Benchmark,
   b) NIST,
   c) ISO 27001.
3.14. System musi umożliwiać :
   a) automatyczne wykonywanie akcji po wykryciu incydentu,
   b) blokowanie adresów IP,
   c) wywoływanie skryptów,
   d) wysyłanie powiadomień,
   e) integrację z systemami zgłoszeniowymi.
3.15. System musi umożliwiać :
   a) tworzenie własnych dashboardów,
   b) tworzenie raportów okresowych,
   c) eksport danych do PDF, CSV,
   d) raportowanie dla kierownictwa,
   e) raportowanie dla audytorów.
3.16. Rozwiązanie musi :
   a) Umożliwiać wdrożenie w infrastrukturze Zamawiającego,
   b) działać w środowisku wirtualnym,
   c) wspierać wysoką dostępność (HA),
   d) wspierać architekturę rozproszoną.
3.17. Bez konieczności wymiany platformy system musi obsługiwać co najmniej :
   a) 1000 monitorowanych stacji roboczych,
   b) 200 serwerów,
   c) 50 urządzeń sieciowych,
   d) 5000 EPS (Events Per Second),
3.18. System musi zapewnić przechowywanie danych przez minimum 12 miesięcy online, możliwość archiwizacji przez minimum 5 lat, a także szyfrowanie danych w spoczynku i transmisji
3.19. Oferowane rozwiązanie musi zostać wdrożone w architekturze wysokiej dostępności (High Availability – HA), zapewniającej ciągłość działania systemu w przypadku awarii pojedynczego węzła.
3.20. System musi zostać uruchomiony na co najmniej dwóch serwerach lub węzłach zapewniających wysoką dostępność (HA) w architekturze active-active, active-passive lub równoważnej.
3.21. Architektura rozwiązania musi umożliwiać:
   a) automatyczne przejęcie funkcji przez drugi węzeł w przypadku awarii jednego z serwerów;
   b) zachowanie ciągłości monitorowania zdarzeń bezpieczeństwa;

c) brak utraty danych telemetrycznych i logów podczas przełączenia awaryjnego;

d) automatyczną synchronizację konfiguracji pomiędzy węzłami klastra.

3.22. Awaria pojedynczego serwera nie może powodować:

a) niedostępności systemu dla administratorów,

b) utraty zdolności do gromadzenia logów,

c) utraty zdolności do generowania alertów bezpieczeństwa,

d) utraty zgromadzonych danych.

3.23. Rozwiązanie musi umożliwiać wykonywanie prac serwisowych, aktualizacji oraz czynności administracyjnych na jednym z węzłów bez konieczności wyłączania całego systemu.

3.24. Zamawiający wymaga, aby architektura zapewniała ciągłość monitorowania, gromadzenia logów, generowania alertów oraz dostęp administracyjny w przypadku awarii pojedynczego węzła.

3.25. Wykonawca zobowiązany jest do przeprowadzenia i udokumentowania testów przełączenia awaryjnego (failover) podczas odbioru rozwiązania.

3.26. Wdrożenie systemu będzie następowało etapami :

ETAP I Projektowanie rozwiązania, w ramach którego Wykonawca przeprowadzi analizę środowiska Zamawiającego oraz przygotuje projekt wdrożenia obejmujący co najmniej:

a) analizę istniejącej infrastruktury teleinformatycznej,

b) identyfikację źródeł logów oraz systemów przeznaczonych do integracji,

c) określenie zakresu monitorowania bezpieczeństwa,

d) opracowanie architektury wdrożenia wraz z rozmieszczeniem komponentów systemu,

e) określenie sposobu integracji z istniejącymi systemami bezpieczeństwa,

f) przygotowanie harmonogramu wdrożenia,

g) uzgodnienie z Zamawiającym planu realizacji prac.

Efektem etapu będzie dokument projektowy zaakceptowany przez Zamawiającego.

ETAP II Instalacja i konfiguracja rozwiązania, w ramach którego Wykonawca zobowiązany jest do:

a) instalacji wszystkich komponentów oferowanego rozwiązania,

b) konfiguracji serwerów zarządzających oraz komponentów analitycznych,

c) wdrożenia agentów na wskazanych serwerach i stacjach roboczych,

d) konfiguracji zbierania logów z systemów określonych w niniejszym OPZ,

e) integracji z systemami bezpieczeństwa, w szczególności zaporami sieciowymi, systemami EDR, systemami kopii zapasowych oraz pozostałymi wskazanymi przez Zamawiającego,

f) konfiguracji mechanizmów korelacji zdarzeń,

g) uruchomienia dashboardów, raportów oraz mechanizmów powiadamiania,

h) przeprowadzenia testów funkcjonalnych i potwierdzenia poprawności działania systemu.

ETAP III Okres obserwacji i optymalizacji, w ramach którego Wykonawca zobowiązany jest do:

a) bieżącej analizy generowanych alertów,

b) optymalizacji reguł korelacyjnych i detekcyjnych,

c) dostosowania progów alarmowych do charakterystyki środowiska Zamawiającego,

d) eliminowania fałszywych alarmów (False Positive),

e) ograniczania przypadków niewykrycia rzeczywistych zagrożeń (False Negative),

f) aktualizacji konfiguracji zgodnie z obserwowanymi zagrożeniami,

g) konsultacji z administratorami Zamawiającego dotyczących jakości wykrywania incydentów.

Po zakończeniu okresu optymalizacji Wykonawca przedstawi raport zawierający co najmniej:

a) opis wykonanych zmian konfiguracji,

b) zestawienie wdrożonych reguł detekcyjnych,

c) analizę najczęściej występujących alertów,

d) rekomendacje dotyczące dalszego rozwoju systemu

3.27. Oferowane rozwiązanie musi być dostarczone w modelu licencji bezterminowej (perpetual license), zapewniającej Zamawiającemu nieograniczone czasowo prawo do użytkowania wszystkich dostarczonych komponentów systemu.

3.28. Licencja bezterminowa musi obejmować wszystkie funkcjonalności wymagane w niniejszym OPZ, bez konieczności ponoszenia dodatkowych opłat abonamentowych warunkujących dalsze korzystanie z systemu.

3.29. W przypadku zakończenia okresu wsparcia technicznego Zamawiający zachowuje pełną możliwość dalszego użytkowania wdrożonego systemu wraz z wszystkimi skonfigurowanymi funkcjonalnościami.

3.30. Licencja musi umożliwiać instalację i eksploatację rozwiązania w infrastrukturze teleinformatycznej Zamawiającego bez obowiązku korzystania z usług chmurowych producenta.

3.31. Zamawiający wymaga, aby licencjonowanie nie było uzależnione od wolumenu przechowywanych logów, liczby analizowanych zdarzeń lub ilości danych retencjonowanych w systemie.

3.32. Wykonawca przeprowadzi szkolenie dla minimum 3 administratorów obejmujące:

a) administrację systemem,

b) tworzenie reguł detekcyjnych,

c) analizę incydentów,

d) tworzenie raportów,

e) obsługę modułów podatności i zgodności

3.33. Wykonawca zapewni wsparcie techniczne przez minimum12 miesięcy.

4. Zakres wdrożenia i konfiguracji środowiska Microsoft 365 :

4.1. Dostarczenie subskrypcji: Microsoft Exchange Online Plan 1: 100 szt. oraz Microsoft Defender for Office Plan 1: 50 szt.

4.2. Utworzenie i konfiguracja dzierżawy (tenant) dla Zamawiającego

4.3. Utworzenie (hardening) konfiguracji dzierżawy Microsoft 365 zgodnie z dobrymi praktykami bezpieczeństwa Microsoft.

4.4. Konfiguracja środowiska hybrydowego łączącego lokalną infrastrukturę Active Directory i Entra ID oraz Exchange Server 2016 z usługami Microsoft Exchange Online.

4.5. Konfiguracja synchronizacji tożsamości z wykorzystaniem Microsoft Entra Connect i wdrożenie logowania jednokrotnego (SSO),

4.6. Konfiguracja polityk bezpieczeństwa w ramach posiadanych przez zamawiającego licencji

4.7. Utwardzenie (hardening) usług Exchange Online Protection (EOP);

4.8. Przygotowanie i wdrożenie rekordów DNS dla usług pocztowych (MX, DKIM,SPF, DMARC, Autodiscover oraz innych wymaganych dla wdrażanych usług)

4.9. Wdrożenie Microsoft Defendera for Office Plan 1 dla 50 użytkowników

4.10. Wdrożenie polityk zagrożeń (Threat Policies) w tym:

a) Anty-spam,

b) Anty-phising

c) Safe-Links

d) Safe-Attachments

4.11. Wdrożenie uwierzytelniania certyfikowanego Microsoft Entra Certificate-Based Authentication (CBA) dla 100 użytkowników wraz z konfiguracją polityk uwierzytelniania.

a) Wdrożenie PKI w lokalnej domenie,

b) Przygotowanie szablonu certyfikatu,

c) Przygotowanie polityk GPO pod certyfikaty,

d) Konfiguracja EntraID i metod MFA.

4.12. Migracja danych, która obejmować będzie:

a) Utworzenie środowiska hybrydowego Exchange Server + Exchange Online,

b) Rekonfigurację usług Exchange zgodnie z projektem migracji,

c) Zmiana przepływu SMTP

d) Wsparcie w konfiguracji połączeń sieciowych,

e) Migrację ok. 100 skrzynek pocztowych (użytkowników i współdzielonych) z Exchange 2016 do Exchange Online,

4.13. Przeprowadzenie procesu wycofania z eksploatacji serwerów Exchange Server 2016 zgodnie z zaleceniami Microsoft, obejmującego m/in. usunięcie baz danych, migrację ról oraz odinstalowanie serwerów.

4.14. Przeprowadzenie szkoleń dla administratorów (3 osób, 8 godzin szkoleniowych, forma zdalna) oraz dla pracowników (do 100 osób w 5 grupach po ok. 20 osób, po 4 godzin szkoleniowych, forma zdalna).

4.15. Przekazanie dokumentacji technicznej i powykonawczej.

5. Wszystkie rozwiązania objęte przedmiotem zamówienia muszą być zgodne z aktualnymi wymaganiami bezpieczeństwa i umożliwiać bezpieczną eksploatację w jednostce sektora publicznego oraz muszą umożliwiać tworzenie kont administracyjnych oraz nadawanie uprawnień zgodnie z zasadą minimalnych uprawnień.

6. Wykonawca zobowiązany jest skonfigurować rozwiązania w sposób ograniczający zbieranie danych do zakresu niezbędnego dla osiągnięcia celów bezpieczeństwa i zgodności z przepisami, a także z uwzględnieniem zasady ochrony danych osobowych, w szczególności minimalizację danych, ograniczenie celu, poufność, integralność, rozliczalność oraz adekwatny poziom zabezpieczeń.

7. Wykonawca wykona prace w sposób niepowodujący nieuzasadnionych przerw w działaniu podstawowych usług Zamawiającego.
8. Wykonawca wykona prace w sposób niepowodujący nieuzasadnionych przerw w działaniu podstawowych usług Zamawiającego.
9. Wszelkie prace mogące wpływać na ciągłość działania systemów produkcyjnych muszą zostać uzgodnione z Zamawiającym z odpowiednim wyprzedzeniem.
10. Interfejsy administracyjne, komunikaty użytkownika lub dokumentacja użytkowa powinny być dostępne w języku polskim, o ile dla danego rozwiązania jest to technicznie dostępne.
11. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają następujące warunki:
    11.1. Wykonawca musi posiadać (lub zobowiązać się do posiadania na dzień podpisania umowy) aktywny status Partner Microsoft;
    11.2. Wykonawca w okresie ostatnich 3 lat musi posiadać zrealizowane co najmniej 3 wdrożenia Microsoft 365 dla min. 100 użytkowników każde, w tym co najmniej 1 w jednostce sektora finansów publicznych;
    11.3. Wykonawca musi posiadać wdrożony i aktywny certyfikowany System Zarządzania Bezpieczeństwem Informacji zgodny z normą ISO/IEC 27001;
    11.4. Wykonawca skieruje do realizacji zamówienia 3 osoby posiadające minimum 2 certyfikaty z:
        a. Microsoft 365 Endpoint Administrator
        b. Microsoft Certified: Cybersecurity Architect Expert
        c. Microsoft Certified: Azure Solutions Architect Expert

CZĘŚĆ II

1. Ogólne parametry agregatu prądotwórczego:
    1.1. Obudowa dźwiękochłonna, wyciszona specjalną, niepalną pianką wygłuszającą, malowana na kolor RAL 1001, z niezbędnymi drzwiami dostępowymi i serwisowymi.
    1.2. Moc znamionowa – 68 kVA (55 kW).
    1.3. Moc awaryjna nie mniej niż – 75 kVA (60 kW).
    1.4. Napięcie – 400/230 V.
    1.5. Częstotliwość – 50Hz.
    1.6. Dostarczone urządzenie powinno być w całości spreparowane przez jednego producenta posiadającego:
        a) wdrożony system ISO 9001,
        b) wdrożony system ISO 14001,
        c) wdrożony system ISO 45001,
        d) wdrożony system ISO 27001.
    1.7. Konstrukcja z możliwością transportu wózkiem widłowym, dźwigiem, HDS – na pasach, widłach lub łańcuchach.
    1.8. Klasa wykonania – G3.
    1.9. Zewnętrzny przycisk zatrzymania awaryjnego.
    1.10. Zaciski na listwie sterowniczej:

a) NC do podłączenia zewnętrznego stopu pożarowego,

b) dla kabla potrzeb własnych agregatu.

1.11. Wysokowydajne amortyzatory drgań silnika i prądnicy.

1.12. Wymiary nie przekraczające (dł. x szer. x wys.) – 2300 x 1000 x 1350 [mm] .

1.13. Zbiornik paliwa co najmniej 100L w ramie agregatu, pozwalający na ciągłą pracę:

a) przy 75% obciążeniu co najmniej 8,4h

b) przy 100% obciążeniu co najmniej 6,4h

1.14. Alarm poziomu paliwa 15% (rezerwa).

1.15. Wyłączenie agregatu przy 5% paliwa (zabezpieczenie przed zapowietrzeniem).

1.16. Wymagany również korek spustowy zbiornika oraz co najmniej jeden niezależny, otwór w zbiorniku zaślepiony deklem na śrubach, umożliwiający montaż i podłączenie dodatkowej.

1.17. Instalacji paliwowej lub przeniesienie wlewu paliwa na drugą stronę zbiornika.

1.18. Stalowy tłumik dźwięków -35db(A) – zabudowany wewnątrz agregatu

2. Parametry silnika:

c) Diesel wolnossący,

d) Liczba i układ cylindrów: 4,

e) Wymagany typ wtrysku – bezpośredni.

f) Elektroniczna regulacja obrotów.

g) Podgrzewanie bloku – grzałka silnika kontrolowana przez sterownik agregatu.

h) Spalanie przy 75% obciążenia nie więcej niż – 11,9 l/h.

i) Spalanie przy 100% obciążenia nie więcej niż – 15,6 l/h.

j) Wlew paliwa - korek zamykany kluczykiem, wewnątrz obudowy.

k) Filtr powietrza suchy.

l) Silnik chłodzony glikolem.

m) Prędkość obrotowa – 1500 r.p.m.

n) Układ elektryczny 12V.

o) Akumulator 12V.

p) Automatyczna ładowarka buforowa akumulatora/ów w czasie czuwania.

q) Osłona elementów gorących oraz ruchomych.

r) Wymagany przepływ spalin 12,3 m3/min

s) Temperatura spalin poniżej 600^0C

3. Parametry prądnicy:

3.1. Automatyczna regulacja napięcia,

3.2. Obudowa (wg IEC-34-5) - IP23.

3.3. Złącze – elastyczny dysk.

3.4. Klasa izolacji – H.

3.5. Wymagane wykonanie: stojan prądnicy powinien być nawinięty z poskokiem 2/3, w celu

uniknięcia krotności trzeciej harmonicznej (3, 9, 15, itd.) napięcia wyjściowego. Zastosowanie podskoku 2/3 ma za zadanie minimalizację indukowania się nadmiernych prądów w obwodzie neutralnym.

3.6. Wytrzymałość zwarciowa prądnicy >300% obciążenia znamionowego.

4. Parametry sterownika:

4.1. Obsługa 400 Hz,

4.2. Dziennik - 400 zdarzeń,

4.3. Możliwość edycji wszystkich parametrów na panelu przednim,

4.4. 3-poziomowe hasło konfiguracyjne,

4.5. Graficzny wyświetlacz LCD 128x64,

4.6. Języki do pobrania (domyślnie – polski),

4.7. Wyświetlanie przebiegów napięcia i prądów,

4.8. Analiza harmonicznych,

4.9. Wyjścia 16 A MCB i GCB,

4.10. 8 konfigurowalnych wejść cyfrowych,

4.11. Wejścia rozszerzalne do 40,

4.12. 6 konfigurowalnych wyjść cyfrowych,

4.13. Wyjścia z możliwością rozszerzenia do 38,

4.14. 3 konfigurowalne wejścia analogowe,

4.15. Zarówno CANBUS-J1939, jak i MPU,

4.16. 3 konfigurowalne alarmy serwisowe,

4.17. Tygodniowy harmonogram pracy,

4.18. Ręczna „precyzyjna regulacja prędkości” w wybranych ECU,

4.19. Automatyczne sterowanie pompą paliwa

4.20. Ochrona przed nadmierną mocą

4.21. Odwrotna ochrona zasilania

4.22. Zabezpieczenie przed przeciążeniem IDMT

4.23. Zrzut obciążenia, obciążenie zastępcze

4.24. Zarządzanie wieloma obciążeniami

4.25. Zabezpieczenie od asymetrii prądu

4.26. Ochrona przed asymetrią napięcia

4.27. Zegar czasu rzeczywistego z podtrzymaniem bateryjnym

4.28. Kontrola prędkości biegu jałowego

4.29. Ładowanie akumulatora włączone

4.30. Wiele parametrów nominalnych

4.31. Napęd Tactor i MCB

4.32. 4 kwadrantowe liczniki mocy agregatu

4.33. Liczniki zasilania sieciowego

4.34. Wskazania poziomu paliwa

4.35. Wyświetlacz diagnostyczny modemu

4.36. Konfigurowalny przez USB, RS-485 i GPRS

4.37. Darmowy program konfiguracyjny

4.38. Gotowy do centralnego monitorowania

4.39. Obsługa mobilnych agregatów prądotwórczych

4.40. Łatwa aktualizacja oprogramowania sprzętowego USB

4.41. Stopień ochrony IP65 ze standardową uszczelką

4.42. Pełna obsługa rozwiązań producenta.

4.43. Komunikaty w języku polskim.

4.44. Kontrola parametrów sieci i agregatu (napięć , prądów, mocy, częstotliwości, cosφ, napięcia ładowania akumulatora, ilość paliwa w zbiorniku, czasu pracy agregatu, parametrów silnika).

4.45. Panel sterownika wyposażony w tabliczkę z diodami sygnalizacyjnymi dla łatwej obsługi i szybkiej identyfikacji stanów pracy urządzenia. Wymagana jest identyfikacja alarmów dotyczących działania baterii, pracy alternatora, poziomu paliwa, ciśnienia oleju oraz dwa dodatkowe do zdefiniowania. Sterownik musi posiadać w tylnej ścianie wolne sloty do podłączenia dodatkowych modułów sygnalizacyjnych np. GSM, ETHERNET, styków/wyjść przekaźnikowych dla sygnałów bezpotencjałowych (do zdefiniowania przez użytkownika)

4.46. Możliwość wyświetlania pomiarów :

a) Napięcia sieci i agregatu PN / PP

b) Częstotliwość sieci i agregatu

c) Prądy fazowe sieci i agregatu

d) Prądy neutralne sieci i agregatu

e) Sieć i agregat, faza i suma, kW, kVA, kVAr, pf

f) Prędkość silnika

g) Napięcie baterii

h) Temperatura silnika

i) Ciśnienie oleju

j) Zużycie paliwa (dla silników wyposażonych w ECU)

4.47. Możliwości komunikacji :

a) 4 - pasmowy modem GPRS - opcjonalnie

b) Port USB

c) RS-485 (2400-115200) - opcjonalnie

d) RS-232 (2400-115200)

e) J1939-CANBUS

f) Centralny monitoring internetowy

g) Wysyłanie wiadomości SMS - opcjonalnie

h) Wysyłanie e-mail - opcjonalnie

i) Modbus RTU

4.48. Szafa elektryczna/automatyki agregatu zbudowana na podzespołach renomowanych producentów elektryki i elektroniki, według norm i standardów.

5. Wymagane jest, aby agregat pochodził z seryjnej i bieżącej produkcji, wyprodukowany w Polsce, posiadał oznaczenie CE, serwis oraz magazyn części zamiennych i materiałów eksploatacyjnych na terenie Polski.
6. Zamawiający nie dopuszcza modyfikacji urządzenia ingerującego w jego konstrukcję.
7. Transport i rozładunek agregatu w wskazanym podczas wizji lokalnej miejscu tj. obok bramy do archiwum na istniejącej kostce brukowej.
8. Wykonawca ma obowiązek przeprowadzić szkolenie z obsługi sprzętu dla wskazanych przez Zamawiającego pracowników.
9. Zamawiający wymaga ogrodzenia i zadaszenia przestrzeni wokół agregatu za pomocą przęseł modułowych w celu ochrony przed atakami wandalizmu.
10. Wykonawca udzieli gwarancji na sprzęt na okres minimum 5 lat.