



Załącznik nr 1: Szczegółowy opis parametrów technicznych i funkcjonalności

I. Cel:

Zamawiający planuje zakup licencji na platformę programową HPE Networking IMC Enterprise Software Platform with 50-node License E-LTU zwanej dalej Oprogramowaniem,
dla Państwowej Inspekcji Pracy Głównego Inspektoratu Pracy

W ramach realizacji zamówienia, Wykonawca dostarczy następujące oprogramowanie Hewlett Packard Enterprise:

LP.	Nazwa produktu	Numer produktu (SKU)	Liczba
1	Elektroniczna dostawa licencji bezterminowej na HPE IMC Enterprise Edition Software Platform with 50-Node E-LTU	JG748AAE	1

Zamawiający informuje, że:

- posiada środowisko sieciowe składające się z niżej wymienionych modeli urządzeń sprzętowych którymi będzie zarządzał Oprogramowaniem (SKU i nazwa urządzenia):
 - J8698A HPE Aruba Networking 5412R zl2 Switch
 - J8700A HP 5412-96G zl Switch
 - J9782A Aruba 2530-24 Switch (J9782A)
 - J9821A HPE Aruba Networking 5406R zl2 Switch
 - J9827A HPE Aruba Networking 5400R zl2 Management Module
 - JD022A HP 1405-24G Switch
 - JE005A HP 1910-16G Switch
 - JE006A HP 1910-24G Switch
 - JG539A HPE 1910 24 PoE+ Switch
 - JG920A HPE 1920 8G Switch
 - JG928A HPE 1920 48G PoE+ (370W) Switch
 - JL075A Aruba 3810M 16SFP+ 2-slot Switch
 - JL084A JL253A Aruba 2930F 24G 4SFP+ Switch
 - JL256A HPE Aruba 2930F 48G PoE+ 4SFP+ Switch
 - JL386A HPE 1920S 48G 4SFP PPOE+ 370W Switch
 - JL676A HPE Aruba Networking CX 6100 48G 4SFP+ Switch
- posiada środowisko wirtualizacyjne Microsoft Hyper-V;



Zamawiający wymaga dostarczenia licencji w terminie 14 dni kalendarzowych od dnia podpisania umowy ważnej bezterminowo.

II. Zamawiający dopuszcza zaoferowanie pakietów równoważnych do Oprogramowania.

Jeżeli Zamawiający określił w OPZ wymagania z użyciem nazw własnych produktów lub marek producentów, w szczególności w obszarze specyfikacji przedmiotu zamówienia, to należy traktować wskazane produkty jako rozwiązania wzorcowe. W każdym takim przypadku Zamawiający oczekuje dostarczenia produktów wzorcowych albo równoważnych, spełniających poniższe warunki równoważności.

1. W przypadku dostarczania oprogramowania równoważnego względem wyspecyfikowanego przez Zamawiającego w OPZ, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w OPZ, w szczególności w zakresie:
 - warunków licencji/sublicencji w każdym aspekcie licencjonowania/ sublicencjonowania, które muszą być identyczne lub rozszerzone, przy czym rozszerzony zakres musi zawierać również wszystkie elementy licencjonowania,
 - funkcjonalności równoważnej oprogramowania, która nie może być gorsza od funkcjonalności wymienionych w rozdziale III „Opis wymagań minimalnych dla licencji równoważnej” oraz w rozdziale I, gdzie kody produktu wzorcowego definiują funkcjonalności, jakie musi spełnić produkt równoważny,
 - oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego,
 - oprogramowanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie.
2. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego, również po usunięciu oprogramowania równoważnego.
3. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia/gwarancji producentów używanego i współpracującego z nim sprzętu i oprogramowania u Zamawiającego.
4. Oprogramowanie równoważne dostarczone przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia.

5. W przypadku dostawy oprogramowania równoważnego Wykonawca zobowiązany jest:
 - dostarczyć oprogramowanie równoważne w terminie do 14 dni od dnia podpisania Umowy,
 - dostarczyć wszelkie dodatkowe licencje - niezbędne do prawidłowego funkcjonowania oprogramowania równoważnego.
6. Dostarczona licencja na oprogramowanie równoważne musi obejmować co najmniej jedną instancję serwera zarządzającego i co najmniej 50 urządzeń sieciowych. Licencja nie może mieć ograniczeń w liczbie dostępów do konsoli zarządzającej.

III. Opis wymagań minimalnych dla licencji równoważnej:

Zamawiający wymaga dostarczenia bezterminowej licencji na oprogramowanie w terminie 14 dni roboczych od podpisania umowy.

1. Oprogramowanie musi pozwalać na kompleksowe zarządzanie urządzeniami sieciowymi w modelu FCAPS: Fault, Configuration, Administration, Performance, Security, czyli zarządzać obszarami:
 - a. Awaryjne – alarmy, dziennik systemowy i funkcje pułapek
 - b. Konfiguracja – centrum konfiguracji, zgodność, VLAN i menedżer ACL
 - c. Administrowanie – zasoby sieciowe
 - d. Wydajność – zarządzanie wydajnością i zarządzanie siecią wirtualną
 - e. Bezpieczeństwo – centrum kontroli bezpieczeństwa
2. Oprogramowanie musi obsługiwać model ITIL Operational Center of Excellence w zakresie praktyk IT
3. Oprogramowanie musi wykorzystywać paradygmat zarządzania z jednym panelem, aby umożliwić kompleksowe zarządzanie usługami IT
4. Oprogramowanie musi zapewniać skalowalność poprzez obsługę rozproszonej i hierarchicznych architektury systemowej, dzięki dodatkowemu wsparciu systemu operacyjnego i bazy danych.
5. Oprogramowanie musi wykorzystywać model SOA (Service Oriented Architecture), aby zapewnić pełne zarządzanie zasobami, usługami i użytkownikami.
6. Oprogramowanie musi umożliwiać integrację oddzielnych narzędzi zarządzania dzięki modułowej konstrukcji.
7. Oprogramowanie musi umożliwiać przedsiębiorstwu rozszerzenie skali zarządzania infrastrukturą i jednocześnie płynne wdrażanie nowych technologii.
8. Oprogramowanie musi być zgodne z systemami Microsoft® Windows® Server oraz Red Hat Linux i obsługiwać zarządzanie urządzeniami Hewlett Packard Enterprise i innych producentów.
9. Oprogramowanie musi posiadać, potwierdzoną przez firmę Hewlett-Packard, informację o zgodności z przełącznikami Hewlett-Packard i braku ograniczeń gwarancyjnych.
10. Oprogramowanie musi posiadać bibliotekę dokumentacji i bazy wiedzy.
11. **Interfejs użytkownika:** Interfejs użytkownika na pulpicie ma oferować minimum osiem konfigurowalnych interfejsów ekranowych opartych na ikonach, które można uporządkować według konkretnych zadań umożliwiających administratorom i operatorom zarządzanie

infrastrukturą sieciową. Interfejs ma zapewniać również różne ścieżki do tego samego celu.

Operatorzy mają mieć dostęp do kreatorów/przewodników szybkiego startu. Interfejs ma mieć funkcję „Ulubione” dzięki której operatorzy będą mogli tworzyć linki do funkcji, z których korzystają najczęściej.

12. Oprogramowanie musi posiadać co najmniej angielski interfejs językowy.
13. **Zarządzanie zasobami:** Oprogramowanie musi zapewniać kompleksowe zarządzanie urządzeniami wielu dostawców za pomocą jednego panelu. Operatorzy Oprogramowania muszą mieć dostęp do zestawu funkcji do zarządzania i monitorowania wielu różnych urządzeń sieciowych, mogąc nimi zarządzać indywidualnie lub grupowo. Operatorzy muszą mieć możliwość dodawania urządzeń ręcznie, jak i za pomocą pliku CSV lub za pomocą automatycznego wykrywania. Operatorzy muszą mieć możliwość przeglądania urządzeń według topologii, widoku IP, widoku urządzenia i widoku niestandardowego, a także wyświetlać kluczowe szczegóły urządzenia.
14. **Zarządzanie konfiguracją i zmianami:** Oprogramowanie ma umożliwiać dostęp do funkcji zarządzania zmianami i konfiguracją zarządzanych urządzeń. Operatorzy muszą mieć możliwość przeglądania i wdrażania konfiguracji i oprogramowania systemowego na urządzeniach, uzyskiwać dostęp do szablonów konfiguracji, korzystania z biblioteki oprogramowania systemowego, czyszczenia urządzeń pod kątem nowych wdrożeń oraz tworzenia kopii zapasowych zarządzanych systemów.
15. **Monitorowanie i zarządzanie wydajnością:** Oprogramowanie musi umożliwiać monitorowanie wydajności zarządzanych urządzeń. Funkcje zarządzania wydajnością mają umożliwiać dostosowanie gromadzenia, alarmowania i prezentacji danych dotyczących wydajności. System ma umożliwiać zarządzanie wydajnością w czasie rzeczywistym i w historii dla zarządzanych urządzeń, takich jak routery i przełączniki, dla danych z sieci IPsec VPN, WSM i QoS. Ma mieć możliwość dostosowywania ustawień progów, widoków i danych dotyczących wydajności oraz monitorowania globalnego. Oprogramowanie ma umożliwiać podgląd w czasie rzeczywistym.
16. **Zarządzanie wirtualizacją:** Oprogramowanie ma zapewniać wgląd i zarządzanie sieciami wirtualnymi oraz zmniejszać złożoność migracji poprzez dopasowanie i automatyzację zasad sieciowych do obrazów wirtualnych. Ma obsługiwać Hyper-V, KVM i VMware®; oraz automatyczne śledzenie portu dostępu do sieci maszyn wirtualnych.
17. **Elastyczne, scentralizowane raportowanie:** Oprogramowanie musi oferować opcje raportowania wydajności administratora, operatora i zasobów według szablonu. Ma udostępniać raporty w czasie rzeczywistym oraz raporty niestandardowe. Raporty niestandardowe mają mieć możliwość zawierania danych dotyczących urządzeń (adres IP, status, lokalizacja, wersja sprzętu/oprogramowania systemowego) i łączy (status obu końców łącza). Raporty mają mieć możliwość dostosowywania w interfejsie do konkretnych potrzeb Operatorów.
18. **Globalne zarządzanie listami kontroli dostępu (ACL):** Oprogramowanie ma zapewniać operatorom kompleksowy zestaw funkcji do zarządzania listami kontroli dostępu (ACL), w tym przeglądania i konfigurowania list kontroli dostępu na urządzeniach zarządzanych przez Oprogramowanie oraz importowanie list kontroli dostępu. Menedżer ACL ma obsługiwać podstawowe, zaawansowane, łączone i definiowane przez użytkownika listy kontroli dostępu (ACL). Asystent ACL ma ułatwiać tworzenie szablonów reguł ACL i zarządzanie nimi. Lista zasobów ACL udostępnia portal do

przeglądania i zarządzania listami kontroli dostępu (ACL) z listą zestawów reguł. Kreator wdrażania list kontroli dostępu (ACL) wspomaga wdrażanie list kontroli dostępu (ACL).

19. **Kontrola administracyjna oparta na rolach (RBAC):** Oprogramowanie ma zapewniać administratorom zarówno narzędzia, jak i możliwość udzielania dostępu tylko do tych funkcji i zasobów, których potrzebują operatorzy. System ma zapewniać również kontrolę i ścieżki audytu, wspierając najlepsze praktyki zarządzania IT. Uprawnienia zarządzania i dostęp do wszystkich zasobów zarządzanych przez Oprogramowanie mają być przyznawane za pośrednictwem grup operatorów, grup urządzeń i niestandardowych widoków urządzeń. Administrator ma mieć możliwość używania grup operatorów do udzielania lub ograniczania dostępu do różnych funkcji Oprogramowania.
20. **Zarządzanie zgodnością:** Oprogramowanie ma zawierać predefiniowane zasady zgodności, a także umożliwiać konfigurowanie alarmów w przypadku, gdy zarządzane urządzenia nie przejdą kontroli zgodności.
21. **Zarządzanie zasobami sieciowymi:** Administratorzy i operatorzy muszą mieć możliwość śledzenia zasobów, a także zmian w zasobach. Funkcja ta ma zapewniać operatorom dostęp do listy zasobów oraz możliwości przechodzenia do szczegółów poszczególnych urządzeń lub szczegółów audytu urządzeń. Operatorzy mają również mieć możliwość wyszukiwania konkretnych rekordów audytu i zarządzania procesem audytu urządzeń.
22. **Zarządzanie awariami w czasie rzeczywistym:** Oprogramowanie ma integrować system zarządzania siecią, obejmujący awarie, wydajność, audyt, bezpieczeństwo i konfigurację, zmniejszając nakład pracy wymagany do zarządzania złożoną infrastrukturą sieciową, umożliwiając menedżerom sieci korzystanie z jednej bazy danych urządzeń sieciowych, która ma obsługiwać różne zadania zarządzania siecią. Baza danych ma integrować się ze wszystkimi funkcjami Oprogramowania. System zarządzania alarmami lub zdarzeniami ma wykorzystywać istniejącą bazę danych urządzeń i generować alarmy w przypadku wystąpienia zdarzeń interesujących operatorów.
23. **Funkcje niestandardowe i obsługa urządzeń innych firm:** Oprogramowanie ma umożliwiać rozszerzenie funkcji zarządzania i konfiguracji urządzeń. Użytkownicy mają mieć możliwość rozszerzenia istniejących funkcji o obsługę urządzeń innych firm, poprzez skrypty i pliki XML.
24. **Kontrola zabezpieczeń:** Oprogramowanie ma umożliwiać definiowanie zasad i konsekwentne egzekwowanie ustawień na wybranych urządzeniach; ma również używać zasady do zarządzania sieciami VLAN i ustawieniami portów VLAN lub automatycznie stosować szablon konfiguracji na nowo wykrytych urządzeniach. Ma umożliwiać tworzenie zasad alarmujących gdy konfiguracje urządzeń staną się niezgodne.
25. **Gromadzenie danych sieciowych:** Oprogramowanie ma umożliwiać wysyłanie zarchiwizowanych informacji o sieci, urządzeniu lub oprogramowaniu do odpowiednich działów wsparcia w jednym prostym kroku. Ma pozwalać gromadzić wybrane dane i generować raporty oraz pliki danych zawierające odpowiednie informacje. Ma dostarczać raporty do wybranego miejsca docelowego, pocztą elektroniczną, przez FTP, SFTP lub do pliku.
26. **Analiza ruchu sieciowego:** Oprogramowanie ma mieć możliwość informowania operatorów o bieżącym zużyciu przepustowości sieci przez użytkowników. Minimum 5 węzłów z możliwością zwiększenia.



27. **Rozszerzalność i usługi modułowe:** Oprogramowanie ma posiadać otwartą architekturę zorientowaną na usługi (SOA); ma mieć możliwość integracji z oprogramowaniem innych firm, wykorzystując udostępnione interfejsy API.
28. **Kontrola administracyjna:** Oprogramowanie ma obsługiwać bezpieczny dostęp operatora do Portalu poprzez uwierzytelnianie LDAP lub RADIUS, ma umożliwiać przeglądanie aktywności online operatorów, tymczasowe lub stałe rejestrowanie dostępu operatora, dostęp z wykorzystaniem adresów IP, a także ścieżki audytu, które szczegółowo mają opisywać zmiany wprowadzone przez operatorów na urządzeniach w infrastrukturze.
29. **Biblioteka API i aplikacje innych firm:** Oprogramowanie ma posiadać bibliotekę API wykorzystującą implementację RESTful, w celu ułatwienia integrację z aplikacjami Producenta jak i aplikacjami innych firm. Wywołania API mają być dostępne w bibliotece dokumentacji dołączonej do Oprogramowania.
30. **Monitorowanie usług:** Oprogramowanie ma monitorować dostępność i responsywność usług sieciowych za pomocą konfigurowanych sond. Sondy mogą znajdować się na lokalnych i zdalnych agentach i testować usługi z serwerów i urządzeń wybranych podczas konfigurowania sond. Oprogramowanie ma monitorować minimum następujące protokoły: DNS, FTP, HTTP, TCP, UDP, VoIP SMTP, DHCP, ICMP, Radius, TACACS+.
31. **Dostęp przez SSH:** Administrator ma mieć możliwość używania przeglądarki do zdalnego dostępu i zarządzania urządzeniami za pośrednictwem SSH bez konieczności instalowania narzędzia SSH na komputerze klienckim używanym administratora. Obsługuje SSH v1/v2.
32. **Wysoka dostępność:** W przypadku wzrostu wymagań Oprogramowanie ma umożliwiać (jako dodatkowa licencja) wdrożenie wysokiej dostępności (HA) poprzez udostępnienie jednego lub wielu instancji zapasowych serwerów w celu zapewnienia redundancji. Wysoka dostępność może zostać wdrożona we wdrożeniu ze zdalną bazą danych lub współdzieloną pamięcią masową.

Wykonawca ponosi odpowiedzialność cywilną za ewentualne roszczenia osób trzecich wynikające z naruszenia praw autorskich w związku z dostarczeniem licencji.

Zamówienie dofinansowane ze środków Unii Europejskiej, Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności;
Inwestycja: C3.1.1. Cyberbezpieczeństwo - CyberPL , infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo;
Cyberbezpieczeństwo - Cyberbezpieczny Rząd – w ramach projektu pn. „Cyberbezpieczeństwo w PIP”, na podstawie porozumienia o powierzenie grantu o numerze KPOD.05.10- CR.01-001/24/0036/ KPOD.05.10- CR.01-001/25/2025