ZAPYTANIE OFERTOWE NR 1/2025/KPO

Wdrożenie innowacyjnych rozwiązań robotyzacji i cyfryzacji w SM MLEKPOL wykorzystujących sztuczną inteligencję (AI) i zaawansowaną automatykę do optymalizacji procesów produkcyjnych i zwiększenia efektywności przetwarzania mleka UHT.

I. ZAMAWIAJĄCY

Spółdzielnia Mleczarska „MLEKPOL" w Grajewie
ul. Elewatorska 13, 19-203 Grajewo
NIP 719-000-04-25

II. POSTANOWIENIA OGÓLNE

Niniejsze postępowanie („**Postępowanie**") toczy się w trybie zapytania ofertowego, z zachowaniem zasady konkurencyjności, w związku z realizacją projektu pn. **Wdrożenie innowacyjnych rozwiązań robotyzacji i cyfryzacji w SM MLEKPOL wykorzystujących sztuczną inteligencję (AI) i zaawansowaną automatykę do optymalizacji procesów produkcyjnych i zwiększenia efektywności przetwarzania mleka UHT** dofinansowanego ze środków Europejskiego Funduszu Odbudowy (ang. Next Generation EU) w ramach Instrumentu na rzecz Odbudowy i Zwiększania Odporności, Krajowy Plan Odbudowy i Zwiększania Odporności (KPO), Komponent A „Odporność i konkurencyjność gospodarki" Inwestycji: A2.1.1. Inwestycje wspierające robotyzację i cyfryzację w przedsiębiorstwach.

III. PRZEDMIOT ZAMÓWIENIA

1. Zamówienie w ramach realizowanego projektu obejmuje w szczególności dostawę urządzeń sieciowych i oprogramowania wraz z ich montażem i konfiguracją oraz integracją z istniejącą infrastrukturą.
2. Przedmiot zamówienia obejmuje w szczególności:

Zadanie 1:

1) Dostawa wraz z instalacją przełącznika agregacyjnego, przełączników dostępowych 24- i 48-portowych, wkładek SFP.

2) System/y zarządzania przełącznikami i Access Pointami (Network Management System).
3) Autoryzacja 802.1X w sieci LAN.
4) System NAC, autoryzowany dostęp do sieci w warstwie fizycznej, sieciowej i aplikacyjnej.
5) Zarządzanie dostępem uprzywilejowanym (PAM).
6) UTM w celu ochrony brzegu sieci OT.

Zadanie 2:

1) Rozbudowa sieci WiFi.

Zadanie 3:

1) Przełącznik przemysłowy 8-portowy.
2) UTM w celu ochrony brzegu sieci OT.
3) System SIEM.

Uwaga: Ponieważ Przedmiot zamówienia będzie realizowany w pracującym zakładzie, Zamawiający wymaga, aby wszelkie prace zostały wykonane w sposób niezakłócający produkcji na wydziałach produkcyjnych.

2.1 Udzielenie gwarancji i wsparcia oraz rękojmi na okres minimum 24 miesięcy od dnia przekazania przedmiotu danego zadania na podstawie protokołu odbioru końcowego danego zadania.

2.2 Wykonawca wykona przedmiot zamówienia na podstawie ustaleń zapytania ofertowego wraz z załącznikami (w tym wraz z wzorem umowy stanowiącym załącznik 5 do niniejszego zapytania), zgodnie z szczegółowymi wytycznymi Zamawiającego, a także zgodnie z obowiązującymi przepisami szczegółowymi i sztuką techniczno-technologiczną.

2.3 Opis przedmiotu zamówienia stanowi **Załącznik nr 4** do niniejszego zapytania. Oferta musi być zgodna z Opisem przedmiotu zamówienia i wzorem umowy (załącznik nr 5 do niniejszego zapytania).

2.4 Kod CPV:

32424000-1 – Infrastruktura sieciowa
32428000-9 – Modernizacja sieci
32420000-3 – Urządzenia sieciowe
72268000-1 – Usługi dostawy oprogramowania

IV. TERMIN REALIZACJI UMOWY

Termin realizacji zamówienia:

Zadanie nr 1: maksimum 12 tygodni od dnia podpisania umowy,

Zadanie nr 2: maksimum 24 tygodnie od dnia podpisania umowy,

Zadanie nr 3: maksimum 42 tygodni od dnia podpisania umowy, nie później niż do dnia 15.12.2025 r.

V. MIEJSCE REALIZACJI UMOWY

Miejsce realizacji zamówienia: 19-203 Grajewo, ul. Elewatorska 13.

VI. INFORMACJE O CHARAKTERZE PRAWNYM, EKONOMICZNYM, FINANSOWYM I TECHNICZNYM

1. Przedstawienie w ofercie informacji nieprawdziwych mających wpływ na wynik Postępowania będzie skutkować wykluczeniem Wykonawcy z Postępowania i odrzuceniem jego oferty co nie wyłącza dalej idących roszczeń i konsekwencji.
2. Z postępowania o udzielenie zamówienia wykluczeniu podlegają Wykonawcy, którzy są powiązani osobowo lub kapitałowo z Zamawiającym. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru Wykonawcy a Wykonawcą, polegające w szczególności na:
   a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
   b) posiadaniu co najmniej 10 % udziałów lub akcji,
   c) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
   d) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia, lub związanie z tytułu przysposobienia, opieki lub kurateli albo pozostawaniu we wspólnym pożyciu z wykonawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców ubiegających się o udzielenie

zamówienia;

e) pozostawaniu z wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.

Wykonawca zobowiązany jest dołączyć do oferty oświadczenie o braku w/w powiązań według wzoru stanowiącego **Załącznik nr 2** do niniejszego zapytania ofertowego.

3. Wykonawca powinien wykazać, że wykonał należycie, w okresie ostatnich pięciu lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy, w tym okresie podobne instalacje pracujące z pomyślnym skutkiem o podobnych parametrach:
   - minimum dwa zadania polegające na dostawie i wdrożeniu sprzętu i oprogramowania informatycznego, w tym infrastruktury sieciowej, o wartości min. 1 000 000,00 zł brutto.

   Do oferty należy załączyć wykaz dostaw i usług wraz z dokumenty potwierdzające posiadanie odpowiedniego doświadczenia (np. referencje).

   Ocena spełnienia powyższego warunku zostanie dokonana zgodnie z metodą zero-jedynkową – tj. formułą „spełnia – nie spełnia". Oferta Wykonawcy, który nie spełni powyższego warunku zostanie odrzucona.
4. Wykonawca powinien wykazać, że dysponuje potencjałem technicznym i zawodowym niezbędnym do wykonania zamówienia, dotyczącym dysponowania osobami zdolnymi do wykonania zamówienia.

   Wykonawca powinien wykazać, że dysponuje przynajmniej jedną osobą Inżyniera posiadającego doświadczenie we wdrażaniu infrastruktury sieciowej popartej udziałem w minimum 3 zamówieniach oraz posiada certyfikat w zakresie konfigurowania, obsługi i rozwiązywania problemów z sieciami średniej wielkości i korporacyjnymi.

   Do oferty należy załączyć Wykaz osób wraz z dokumentami potwierdzającymi posiadanie odpowiedniego potencjału technicznego.
5. Wykonawca może polegać na zasobach innych podmiotów, niezbędnych do potwierdzenia spełnienia warunków udziału oraz należytego wykonania zamówienia, niezależnie od charakteru prawnego łączących go z nimi stosunków. Wykonawca w takiej sytuacji zobowiązany jest udowodnić Zamawiającemu, iż będzie dysponował zasobami niezbędnymi do realizacji zamówienia, w szczególności przedstawiając w tym celu pisemne

zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonywaniu zamówienia lub inny dokument potwierdzający korzystanie z niezbędnych zasobów podmiotu w formie np. umowy współpracy, umowy licencyjnej.

UWAGA – Wykonawca, który – w celu potwierdzenia spełnienia warunków udziału dotyczących wiedzy i doświadczenia – polega na zasobach innych podmiotów, może skorzystać z przysługującego mu uprawnienia pod warunkiem, że podmioty udostępniające zasoby wykonają prace lub będą świadczyć usługi, do realizacji których te zasoby są wymagane.

Powyższe oznacza, że przy zaistnieniu powyższych okoliczności podmiot udostępniający wskazane zasoby musi być wskazany w treści oferty jako „**podwykonawca**".

W celu oceny, czy Wykonawca polegając na zdolnościach lub sytuacji innych podmiotów będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia oraz oceny, czy stosunek łączący wykonawcę z tymi podmiotami gwarantuje rzeczywisty dostęp do ich zasobów, treść zobowiązania podmiotu trzeciego lub treść innego dokumentu, stanowiących o udostępnieniu określonych zasobów, winna w szczególności wskazywać:

- zakres dostępnych wykonawcy zasobów innego podmiotu;
- sposób wykorzystania zasobów innego podmiotu, przez wykonawcę, przy wykonywaniu zamówienia publicznego;
- zakres i okres udziału innego podmiotu przy wykonywaniu zamówienia publicznego;
- czy podmiot, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje prace lub usługi.

6. Zamawiający zastrzega sobie prawo do odrzucenia oferty zawierającej cenę przekraczającą kwotę, którą Zamawiający planuje przeznaczyć na realizację zamówienia lub niezawierającej dowodu złożenia wadium. Zamawiający zastrzega sobie prawo do odrzucenia oferty, której treść jest niezgodna z zapytaniem ofertowym, w szczególności w przypadku wystąpienia takiej niezgodności z załącznikiem nr 3 – specyfikacja techniczna oraz w sytuacji niezłożenia oferty na wzorcowym formularzu (załącznik nr 1 – formularz

ofertowy).

7. Wykonawca wniesie, przed złożeniem oferty wadium wysokości 400.000,00 PLN (słownie czterysta tysięcy złotych) celem przystąpienia do przetargu oraz ma obowiązek załączyć dowód złożenia wadium do oferty. Wadium może być wniesione w formie:
   a) pieniężnej wpłaconej przelewem na rachunek bankowy Zamawiającego prowadzony przez: BNP Paribas Bank Polska S.A. nr rachunku 97 2030 0045 1110 0000 0018 4890.
8. Wadium podlegać będzie zwrotowi wszystkim, którzy je wpłacili w terminie 45 dni od zawarcia umowy z Wykonawcą który wygra przetarg. Wadium podlega zaś przepadkowi na rzecz Zamawiającego, jeżeli mimo wezwania Wykonawca nie zawrze umowy w zakreślonym terminie.
9. Wykonawca wniesie, przed zawarciem umowy, zabezpieczenie należytego wykonania umowy („**zabezpieczenie**").
10. Zabezpieczenie może być wniesione (według wyboru Wykonawcy) w jednej z następujących form:
    b) pieniężnej – 20 % wartości wynagrodzenia brutto wpłacone przelewem na rachunek bankowy Zamawiającego prowadzony przez: BNP Paribas Bank Polska S.A. nr rachunku 97 2030 0045 1110 0000 0018 4890,
    c) gwarancjach bankowych lub ubezpieczeniowych – 20 % wartości wynagrodzenia brutto.
11. Zabezpieczenie służy pokryciu wszelkich roszczeń z tytułu niewykonania lub nienależytego wykonania Umowy, w tym odszkodowawczych, kar umownych, kosztów wykonania zastępczego itd.
12. W przypadku wniesienia zabezpieczenia należytego wykonania umowy w formie gwarancji, gwarancja musi być co najmniej gwarancją bezwarunkową, nieodwołalną i płatną na pierwsze pisemne żądanie Zamawiającego (nie później niż w ciągu 30 dni od daty zgłoszenia żądania), do której zastosowanie będzie miało prawo polskie, ważną nie krócej niż do wskazanego poniżej terminu wygaśnięcia zabezpieczenia. W treści gwarancji nie mogą być wymienione jakiekolwiek warunki lub dokumenty uzasadniające roszczenie.
13. Zabezpieczenie w formie gwarancji bankowej lub ubezpieczeniowej może wygasnąć nie wcześniej niż według następującego harmonogramu:
    a) 80% wysokości zabezpieczenia w terminie 30 dni od dnia wykonania ostatniego zadania i uznania przez Zamawiającego za należycie wykonany całego przedmiotu umowy, co

zostanie potwierdzone protokołem odbioru techniczno-jakościowego ostatniego zadania i całego przedmiotu umowy bez uwag

b) 20% wysokości zabezpieczenia stanowić będzie zabezpieczenie roszczeń Zamawiającego z tytułu gwarancji na przedmiot umowy – gwarancja bankowa lub ubezpieczeniowa w tym zakresie może wygasną najwcześniej w terminie 15 dni po upływie okresu gwarancji dla całości przedmiotu umowy (wszystkich zadań) i należytym wykonaniu obowiązków gwarancyjnych, co zostanie potwierdzone pogwarancyjnym protokołem odbioru bez uwag.

14. W przypadku zabezpieczenia w formie pieniężnej zostanie ono zwrócone we wskazanych wyżej terminach wygaśnięcia zabezpieczenia. Pozostałe zabezpieczenia zostaną Wykonawcy zwrócone na jego pisemne żądanie złożone po upływie okresu gwarancji.
15. Zamawiający nie dopuszcza składania ofert częściowych. Zamawiający nie dopuszcza składania ofert wariantowych.
16. Zamawiający nie przewiduje udzielenia Wykonawcy zamówień uzupełniających.
17. Umowa (w tym załączniki do umowy) zawarta w wyniku Postępowania, może zostać zmieniona w drodze pisemnego aneksu do umowy w następującym zakresie i przypadkach:
    a) zmiany wynagrodzenia Wykonawcy w stopniu odpowiadającym zmianie stawki podatku VAT (+/-), w przypadku zmiany stawki podatku VAT,
    b) zmiany terminu wykonania zamówienia (w tym terminów pośrednich), w przypadku gdy konieczność zmiany terminu wykonania umowy wynika z przyczyn niezależnych od Wykonawcy lub z potrzeb Zamawiającego uzasadnionych celami projektu;
    c) zmiany warunków i terminów płatności wynagrodzenia, w przypadku gdy konieczność zmiany wynikać będzie z przyczyn niezależnych od Wykonawcy lub z potrzeb Zamawiającego uzasadnionych celami projektu;
    d) zmiany zakresu rzeczowego przedmiotu zamówienia poprzez jego ograniczenie przy odpowiedniej zmianie wynagrodzenia Wykonawcy, w przypadku, gdy konieczność takiej zmiany wynika (i) ze zdarzeń lub okoliczności uniemożliwiających lub utrudniających realizację zamówienia zgodnie z ofertą Wykonawcy albo (ii) z przyczyn niezależnych od Wykonawcy albo (iii) z potrzeb Zamawiającego uzasadnionych celami projektu; zmiany sposobu i/lub metody realizacji zamówienia, w przypadku, gdy konieczność takiej zmiany wynika (i) ze zdarzeń lub okoliczności uniemożliwiających lub utrudniających realizację zamówienia zgodnie z ofertą Wykonawcy albo (ii) z

przyczyn niezależnych od Wykonawcy albo (iii) z potrzeb Zamawiającego uzasadnionych celami projektu;

e) zmiany (i) zakresu rzeczowego przedmiotu zamówienia i/lub (ii) wynagrodzenia Wykonawcy i/lub (iii) terminu realizacji zamówienia, w tym także terminów pośrednich i/lub (iv) sposobu i/lub metody realizacji zamówienia, w przypadku ograniczenia środków finansowych przez stosowną instytucję zarządzającą/ wdrażającą / pośredniczącą etc.

f) zmiany (i) zakresu rzeczowego przedmiotu zamówienia i/lub (ii) terminu realizacji zamówienia, w tym także terminów pośrednich, (iii) sposobu i/lub metody realizacji zamówienia, i/lub (iv) wynagrodzenia Wykonawcy, w przypadku uzgodnień Zamawiającego z instytucją zarządzającą/ wdrażającą / pośredniczącą etc. co do zakresu lub sposobu realizacji projektu lub w przypadku narzucenia przez instytucję zarządzającą/wdrażającą/pośredniczącą konieczności dokonania zmian lub wymagań albo innych zaleceń etc.

g) zmiany (i) zakresu rzeczowego przedmiotu zamówienia i/lub (ii) terminu realizacji zamówienia, w tym terminów pośrednich i/lub (iv) sposobu i/lub metody realizacji zamówienia, i/lub (v) zasad odbioru etc. i/lub (vi) wynagrodzenia Wykonawcy, w przypadku zmian technicznych i/lub organizacyjnych po stronie Zamawiającego i/lub zmian wytycznych dotyczących realizacji projektów współfinansowanych ze środków europejskich lub przepisów prawa dotyczących realizacji projektu.

14. Nie stanowi zmiany umowy, w rozumieniu punktu powyżej:

a) zmiana danych związanych z obsługą administracyjno-organizacyjną umowy (np. zmiana nr rachunku bankowego, zmiana danych teleadresowych);

b) zmiana firm (nazw) stron lub ich formy prawnej (przy zachowaniu ciągłości prawnej).

VII. SPOSÓB PRZYGOTOWANIA OFERTY

1. Ofertę sporządzić należy zgodnie z wzorem pn. „Formularz ofertowy” stanowiącym **Załącznik nr 1** do niniejszego zapytania ofertowego, w języku polskim, w formie pisemnej, czytelnie, wypełniając nieścieralnym atramentem lub długopisem, maszynowo lub komputerowo. Oferta winna być podpisana przez Wykonawcę lub osobę upoważnioną do reprezentowania Wykonawcy na dowód czego należy załączyć odpowiednie dokumenty w szczególności aktualny wydruk KRS, pełnomocnictwa. Cała oferta i dokumentacja musi

zostać złożona poprzez bazę konkurencyjności w formie skanów w formacie PDF, ZIP (maksymalnie 20 plików nie większych niż 20 megabajtów każdy). Nie jest dopuszczalny format RAR. Nazwy plików i folderów (katalogów) winny odzwierciedlać w sposób czytelny ich zawartość.

2. Do Formularza ofertowego stanowiącego **Załącznik nr 1** do zapytania ofertowego należy dołączyć:
   a. Oświadczenie o braku powiązań osobowych lub kapitałowych pomiędzy Wykonawcą a Zamawiającym stanowiące **Załącznik nr 2** do zapytania ofertowego,
   b. Aktualny odpis z właściwego rejestru lub centralnej ewidencji i informacji o działalności gospodarczej jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, wystawionego nie wcześniej niż 2 miesiące przed upływem terminu składania oferty,
   c. Oświadczenie, że dostarczane urządzenia są fabrycznie nowe, sporządzone zgodne z wzorem stanowiącym **Załącznik nr 2a** do zapytania ofertowego,
   d. Wypełniony dokument Specyfikacji technicznej, stanowiący **Załącznik nr 3** do zapytania ofertowego,
   e. Dokumenty potwierdzające, że Wykonawca wykonał należycie, w okresie ostatnich pięciu lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy, w tym okresie, zadania określone w rozdziale VI pkt. 3,
   f. Dokumenty potwierdzające, że Wykonawca dysponuje potencjałem technicznym i zawodowym niezbędnym do wykonania przedmiotu zamówienia określone w rozdziale VI pkt.4,
   g. Inne dokumenty, których załączenia do oferty wymaga Zamawiający w ramach niniejszego Postępowania (o których mowa w Opisie Przedmiotu Zamówienia - dalej OPZ),
   h. Potwierdzenie wpłaty wadium wysokości 400.000,00 PLN (słownie czterysta tysięcy złotych).
3. Złożoną ofertę uznaje się za kompletną jeśli zawiera wszystkie wymagane informacje zawarte w zapytaniu ofertowym.
4. Jeżeli Wykonawca nie złożył oświadczeń lub dokumentów określonych w niniejszym zapytaniu ofertowym (przy czym brak złożenia formularza ofertowego, stanowiącego Załącznik nr 1 do zapytania ofertowego, powoduje odrzucenie oferty) lub innych dokumentów lub oświadczeń niezbędnych do przeprowadzenia Postępowania, oświadczenia

lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez Zamawiającego wątpliwości, Zamawiający może (co oznacza, że nie musi) wezwać do ich złożenia, uzupełnienia lub poprawienia lub do udzielania wyjaśnień w terminie przez siebie wskazanym, chyba że mimo ich złożenia, uzupełnienia lub poprawienia lub udzielenia wyjaśnień oferta Wykonawcy podlega odrzuceniu, Wykonawca podlega wykluczeniu albo konieczne jest unieważnienie Postępowania.

5. Każdy dokument składający się na ofertę lub złożony wraz z ofertą sporządzony w języku innym niż polski musi być złożony wraz z tłumaczeniem na język polski.
6. Każdy z Wykonawców może złożyć tylko jedną ofertę. Złożenie więcej niż jednej oferty spowoduje odrzucenie wszystkich ofert złożonych przez Wykonawcę.
7. Oferty są przygotowywane i składane na koszt Wykonawców.

VIII. OPIS SPOSOBU OBLICZENIA CENY OFERTY

1. Wykonawca zobowiązany jest do podania w formularzu ofertowym ceny za realizację przedmiotu zamówienia w całości. Dopuszcza się złożenie oferty w dolarach amerykańskich (USD) lub w euro (EUR), jednak Zamawiający do oceny ofert przyjmie średni kurs NBP z dnia opublikowania zapytania ofertowego i dokona przeliczenia na złote polskie (PLN).
2. Podane w ofercie ceny winny być podane jako netto, zaokrąglone do dwóch miejsc po przecinku oraz jako brutto (powiększone o podatek VAT, jeżeli wystąpi).
3. Cena brutto musi uwzględniać wszystkie wymagania niniejszego zapytania ofertowego oraz obejmować wszelkie koszty związane z terminowym i prawidłowym wykonaniem całości przedmiotu zamówienia oraz warunkami i wytycznymi stawianymi przez Zamawiającego, odnoszącymi się do przedmiotu zamówienia oraz podatek od towarów i usług (nie dotyczy Wykonawców zagranicznych, którzy nie są płatnikami podatku VAT w Polsce).
4. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami od towarów i usług, Zamawiający w celu dokonania oceny oferty doliczy do przedstawionej w niej ceny (netto), podatek od towarów i usług, który Zamawiający miałby obowiązek wpłacić zgodnie z obowiązującymi przepisami.
5. Zamawiający może poprawić omyłki polegające na niezgodności oferty z treścią zapytania ofertowego w przypadku, gdy w dostarczonym przez Wykonawcę formularzu ofertowym wystąpią omyłki, niepowodujące istotnych zmian w treści oferty.

6. Cena dla przedmiotu zamówienia może być tylko jedna, nie dopuszcza się wariantowości cen. Wszelkie upusty, rabaty, winny być od razu ujęte w obliczaniu ceny, tak by wyliczona cena za realizację przedmiotu zamówienia była ceną ostateczną, bez konieczności dokonywania przez Zamawiającego przeliczeń i innych działań w celu jej określenia.
7. Szczegółowe zasady oraz sposób rozliczeń określony został w projekcie umowy, stanowiącym **Załącznik nr 5** do zapytania ofertowego.

IX. KRYTERIA OCENY OFERT, INFORMACJA O WAGACH PROCENTOWYCH PRZYPISANYCH DO POSZCZEGÓLNYCH KRYTERIÓW OCENY OFERT, OPIS SPOSOBU PRZYZNAWANIA PUNKTACJI ZA SPEŁNIENIE DANEGO KRYTERIUM OCENY OFERTY

1. Kryteria oceny ofert:
   a) Cena całkowita netto - 70%
   b) Okres gwarancji i wsparcia (w miesiącach) - 20%
   c) Termin realizacji (w tygodniach) – 10%

2. Wartość punktowa w ramach kryterium „Cena całkowita netto" wyliczona zostanie według następującego wzoru:

$$C = \frac{C_n}{C_b} \times 70$$

gdzie:

C – liczba punktów (z uwzględnieniem wagi kryterium) w kryterium cena całkowita netto,

C_n – najniższa oferowana całkowita cena netto,

C_b – całkowita cena netto badanej oferty.

Końcowy wynik powyższego działania zostanie zaokrąglony do dwóch miejsc po przecinku.

3. Wartość punktowa w ramach kryterium „Okres gwarancji i wsparcia (w miesiącach)" przyznana zostanie według następującego wzoru:

$$G = \frac{G_o}{G_{max}} \times 20$$

gdzie:

G – liczba punktów (z uwzględnieniem wagi kryterium) w kryterium Okres gwarancji i wsparcia,

G_o – liczba punktów przyznanych ofercie za Okres gwarancji i wsparcia (równa liczbie miesięcy w ocenianej ofercie),

G_{max} – maksymalna możliwa liczba punktów za Okres gwarancji i wsparcia (równa liczbie miesięcy z oferty Wykonawcy, który zaoferował najdłuższy okres gwarancji i wsparcia).

Końcowy wynik powyższego działania zostanie zaokrąglony do dwóch miejsc po przecinku.
Zamawiający przewidział, że Okres gwarancji i wsparcia (długość okresu gwarancyjnego) nie może być krótszy niż 24 miesiące z zastrzeżeniem dłuższych okresów gwarancyjnych dla wskazanych w Zapytaniu elementów.
Oferta zawierająca jakikolwiek Okres gwarancji i wsparcia (długość okresu gwarancyjnego) krótszy niż 24 miesiące zostanie odrzucona. Dla oferty, która nie zawiera deklaracji w zakresie Okresu gwarancji i wsparcia (długości okresu gwarancyjnego) Zamawiający przyjmie, że okres gwarancji i wsparcia wynosi 24 miesiące.

4. Wartość punktowa w ramach kryterium „Termin realizacji (w tygodniach)" wyliczona zostanie według następujących wzorów:

$$T = \frac{T_n}{T_o} \times 10$$

gdzie:

T – liczba punktów (z uwzględnieniem wagi kryterium) w kryterium Termin realizacji,

T_o – liczba punktów przyznanych ofercie za Termin realizacji (równa liczbie tygodni w ocenianej ofercie),
T_n – maksymalna możliwa liczba punktów za Termin realizacji (równa liczbie tygodni z oferty Wykonawcy, który zaoferował najkrótszy Termin realizacji).

Końcowy wynik powyższego działania zostanie zaokrąglony do dwóch miejsc po przecinku.
Zamawiający przewidział, że Termin realizacji nie może być dłuższy niż 42 tygodnie od dnia podpisania umowy, przy czym nie później niż do dnia 15.12.2025 r.
Oferta nie zawierająca terminu realizacji lub zawierająca termin realizacji dłuższy niż powyższy otrzyma 0 punktów.

5. Łączna ocena obejmie sumę punktów uzyskanych przez ofertę w kryteriach określonych w pkt IX.1. Punkty będą liczone z dokładnością do dwóch miejsc po przecinku, zgodnie z następującym wzorem:

   $S_p = C + G + T$

   gdzie:
   S_p – łączna suma punktów,
   C – liczba punktów w kryterium „ Cena całkowita netto”,
   G – liczba punktów w kryterium „Okres gwarancji i wsparcia”,
   T – liczba punktów w kryterium „Termin realizacji”.

6. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymogom zawartym w zapytaniu ofertowym i zostanie oceniona w podanym kryterium wyboru, jako najkorzystniejsza – uzyskując najwyższą liczbę punktów (maks. 100 pkt.).
7. W przypadku odmowy podpisania umowy przez wybranego Wykonawcę, Zamawiający może zawrzeć umowę z Wykonawcą, który spełnia wymagania zapytania ofertowego i którego oferta uzyskała kolejno najwyższą liczbę punktów.
8. Jeżeli Zamawiający nie będzie mógł wybrać najkorzystniejszej oferty ze względu na to, że złożone zostały oferty, które uzyskały taką samą liczbę punktów, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia – w terminie określonym przez

Zamawiającego – ofert dodatkowych. Wykonawcy składając oferty dodatkowe, nie mogą zaoferować cen wyższych niż zaoferowane w złożonych ofertach.

X. MEJSCE I TERMIN SKŁADANIA OFERTY, OSOBA DO KONTAKTU

1. Oferta i cała dokumentacja musi zostać złożona w bazie konkurencyjności w formie skanów w formacie PDF, ZIP (maksymalnie 20 plików nie większych niż 20 megabajtów każdy). Nie jest dopuszczalny format RAR. Nazwy plików i folderów (katalogów) winny odzwierciedlać w sposób czytelny ich zawartość.
2. Oferty należy składać w terminie do 30 dni od momentu upublicznienia niniejszego zapytania ofertowego w bazie konkurencyjności na stronie bazakonkurencyjności.funduszeeuropejskie.gov.pl. Oferty złożone po terminie nie będą rozpatrywane.
3. Wykonawca może przed upływem terminu składania ofert zmienić lub wycofać swoją ofertę.
4. W toku porównania i oceny ofert Zamawiający może (co nie oznacza, że musi) żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert.
5. Wykonawcy pozostają związani ofertą przez okres 90 dni od terminu otwarcia ofert.
   Zapytanie ofertowe zamieszczono na stronie: bazakonkurencyjnosci.funduszeeuropejskie.gov.pl
6. Osoba do kontaktu z Wykonawcami:
   Pan Piotr Piwowarczyk – Kierownik Działu Informatyki,
   tel.: +48 724 720 039 lub +48 86 273 04 00,
   adres e-mail: piotr.piwowarczyk@mlekpol.com.pl

XI. MIEJSCE I TERMIN OTWARCIA OFERT

Otwarcie ofert nastąpi w dzień roboczy po upływie terminu składania (30 dni od upublicznienia na stronie bazakonkurencyjnosci.funduszeeuropejskie.gov.pl) ofert w siedzibie Zamawiającego – Sala konferencyjna, adres: ul. Elewatorska 13, 19-203 Grajewo.

XII. ZAWARCIE UMOWY

Wykonawca zobowiązany jest podpisać umowę oraz dokonać wszelkich związanych z tym obowiązków (w tym przedłożyć zabezpieczenia) w ciągu 10 dni od zawiadomienia o wyborze

jego oferty. W przypadku, jeżeli Wykonawca nie wypełni tego obowiązku wadium podlega przepadkowi na rzecz Zamawiającego, a Zamawiający jest uprawniony do skierowania do Wykonawcy, który złożył kolejną najkorzystniejsza ofertę zawiadomienia o wyborze jego oferty.

XII. INFORMACJE KOŃCOWE

1. Wykonawca będzie miał prawo do zatrudnienia podwykonawców w celu realizacji przedmiotu zamówienia, pod warunkiem uprzedniej zgody Zamawiającego na zatrudnienie podwykonawców w formie pisemnej.
2. Zamawiający zastrzega sobie prawo do anulowania Postępowania, jego unieważnienia lub wprowadzenia zmian do Postępowania w każdym momencie bez podania przyczyny. W takim przypadku Wykonawcy nie przysługują żadne roszczenia względem Zamawiającego.

XIII. WYKAZ ZAŁĄCZNIKÓW

1. Załącznik nr 1 – Formularz ofertowy
2. Załącznik nr 2 – Oświadczenie o braku powiązań osobowych lub kapitałowych pomiędzy Wykonawcą a Zamawiającym
3. Załącznik nr 2a – Oświadczenie, że urządzenie jest fabrycznie nowe
4. Załącznik nr 3 – Specyfikacja techniczna
5. Załącznik nr 4 – Opis przedmiotu zamówienia (OPZ)
6. Załącznik nr 5 – Wzór umowy

Załącznik nr 1 – Formularz ofertowy

…… ……..

Pieczęć Wykonawcy Miejscowość, data

OFERTA

W POSTĘPOWANIU O UDZIELENIE ZAMÓWIENIA NA:

Wdrożenie innowacyjnych rozwiązań robotyzacji i cyfryzacji w SM MLEKPOL wykorzystujących sztuczną inteligencję (AI) i zaawansowaną automatykę do optymalizacji procesów produkcyjnych i zwiększenia efektywności przetwarzania mleka UHT, nr postępowania 1/2025/KPO

ZAMAWIAJĄCY:

Spółdzielnia Mleczarska „MLEKPOL" w Grajewie
ul. Elewatorska 13, 19-203 Grajewo
NIP 719-000-04-25, Regon: 000827780
Nr KRS: 0000045142
Tel./Fax. ……
Adres e – mail……

WYKONAWCA:

Pełna nazwa Wykonawcy ……

Adres ……

NIP…… REGON …….

Nr KRS ……

Tel./Fax. ……

Adres e – mail……

OSOBA UPOWAŻNIONA DO KONTAKTÓW ZE STRONY WYKONAWCY:

Imię i nazwisko osoby upoważnionej do kontaktów ze strony	
Nr telefonu:	
Adres mailowy:	

Działając w imieniu Wykonawcy, w odpowiedzi na zapytanie ofertowe w ramach w/w postępowania o udzielenie zamówienia, przedstawiamy poniższą ofertę na wykonanie całości przedmiotu zamówienia, określonego w zapytaniu ofertowym:

- **cena za realizację przedmiotu zamówienia wynosi (bez podatku VAT):**
  - **Cena całkowita netto: ……..……**

    (słownie ……...……..)
- **należny podatek VAT ……% w wysokości .....,**

  (słownie ..……)
- **całkowita cena za realizację przedmiotu zamówienia (z podatkiem VAT): .....**

  (słownie .....).

*Oferowana cena za realizację przedmiotu zamówienia obejmuje wszystkie koszty niezbędne do zrealizowania przedmiotu zamówienia zgodnie z zapytaniem ofertowym.

Uwaga:

Cena całkowita powinna być podana liczbą oraz słownie z zaokrągleniem do dwóch miejsc po przecinku.

Oświadczamy, że na w/w przedmiot zamówienia udzielamy gwarancji i wsparcia na okres:……. miesięcy.

Oświadczamy, że w/w przedmiot zamówienia zrealizujemy w terminie ……. tygodni od dnia podpisania umowy, nie później jednak niż do dnia 15.12.2025 r.

Oświadczam/y, że oferowane urządzenie/a:

- są fabrycznie nowe, wykonane z materiałów dopuszczonych do stosowania w przemyśle mleczarskim w krajach Unii Europejskiej i Polski,
- wykonane są zgodnie z obowiązującymi w Unii Europejskiej i Polsce przepisami (dyrektywy, normy przedmiotowe, przepisy bhp, przepisy ochrony środowiska itp.), na potwierdzenie powyższego zobowiązuję/emy się dostarczyć deklarację zgodności CE, i niezbędne zaświadczenia (certyfikaty) dotyczące spełnienia norm i dyrektyw przedmiotowych jeśli takowe występują.

Oświadczam/y, iż zapoznałem/liśmy się z warunkami zapytania ofertowego (w tym wzorem umowy) i nie wnoszę/imy do niego żadnych zastrzeżeń oraz zdobyłem/liśmy konieczne informacje i wyjaśnienia do przygotowania oferty.

Oświadczam/y iż uważam/y się za związanego/ych ofertą przez okres **90 dni** kalendarzowych licząc od dnia upływu terminu składania ofert.

Oświadczam/y iż w przypadku wyboru przez Zamawiającego niniejszej oferty zobowiązuję/y się do podpisania umowy w terminie i miejscu wskazanym przez Zamawiającego oraz wniesienia zabezpieczenia należytego wykonania umowy.

Oświadczam/y, że przedmiot oferty zostanie wykonany zgodnie z Opisem przedmiotu zamówienia.

Załącznikami do niniejszej oferty są:

(1)….....

(2)….....

……

(podpis i pieczęć Wykonawcy)

Załącznik nr 2 – Oświadczenie o braku powiązań osobowych lub kapitałowych pomiędzy Wykonawcą a Zamawiającym

…… ……..

Pieczęć Wykonawcy Miejscowość i data

Oświadczenie

Nawiązując do zapytania ofertowego z dnia

……

ja, niżej podpisany

…….

(imię i nazwisko osoby uprawnionej do reprezentowania Wykonawcy)

działając w imieniu i na rzecz:

……

……

(dane Wykonawcy – pełna nazwa i adres firmy)

oświadczam, że:

Wykonawca nie jest powiązany osobowo lub kapitałowo z Zamawiającym, tzn. nie występują żadne powiązania kapitałowe lub osobowe w rozumieniu wzajemnych powiązań między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru Wykonawcy a Wykonawcą, polegające w szczególności na:

a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
b) posiadaniu co najmniej 10 % udziałów lub akcji,
c) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta,

pełnomocnika,

d) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia, lub związanie z tytułu przysposobienia, opieki lub kurateli albo pozostawaniu we wspólnym pożyciu z wykonawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców ubiegających się o udzielenie zamówienia;

e) pozostawaniu z wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.

…….

(podpis i pieczęć Wykonawcy)

Załącznik nr 2a – Oświadczenie, że urządzenie jest fabrycznie nowe

…….. ……..

Pieczęć Wykonawcy Miejscowość i data

Oświadczenie

Nawiązując do zapytania ofertowego z dnia

……

ja, niżej podpisany

…….

(imię i nazwisko osoby uprawnionej do reprezentowania Wykonawcy)

działając w imieniu i na rzecz:

……

……

(dane Wykonawcy – pełna nazwa i adres firmy)

oświadczam, że:

oferowane przez Wykonawcę w ramach w/w postępowania o udzielenie zamówienia urządzenia są fabrycznie nowe, nie są urządzeniami demonstracyjnymi, używanymi, składanymi z używanych części lub modyfikowanymi.

…….

(podpis i pieczęć Wykonawcy)

Załącznik nr 3 – Specyfikacja techniczna

…… ……..

Pieczęć Wykonawcy Data

Specyfikacja techniczna

Zestawienie wymaganych parametrów techniczno-użytkowych

1. Instalacja i konfiguracja dostarczonych produktów, wraz z wykonaniem niezbędnych połączeń sieciowych – połączenie serwerowni podstawowej i zapasowej.
2. Instalacja i konfiguracja oprogramowania zgodnie z zatwierdzonym projektem.
3. Montaż i konfiguracja urządzeń sieci WiFi.
4. Wykonanie i przekazanie pełnej dokumentacji powdrożeniowej.
5. Instruktaże z zakresu wdrożonych produktów i ich konfiguracji.
6. Szkolenia z zakresu wdrożonych produktów.

Szczegółowe zestawienie ilościowe przedmiotu dostawy:

Pozycja dostawy	**Liczba sztuk lub licencji**
Przełącznik agregacyjny	2
Przełącznik dostępowy 24 portowy	28
Przełącznik dostępowy 48 portowy	14
Wkładki SFP	80
System/y zarządzania przełącznikami i Access Pointami (Network Management System)	500 licencji na urządzenia
Autoryzacja 802.1X w sieci LAN	1
System NAC, autoryzowany dostęp do sieci w warstwie fizycznej, sieciowej i aplikacyjnej. Licencja na min. 2500 końcówek	2500 licencji na urządzenia końcowe
Przełącznik przemysłowy 8 portowy	34
UTM w celu ochrony brzegu sieci OT	1
Zarządzanie dostępem uprzywilejowanym	licencja na 100 użytkowników bez limitu urządzeń końcowych/docelowych
System SIEM	500 licencji na urządzenia końcowe
Rozbudowa sieci WiFi – AP zewnętrzne	45
Rozbudowa sieci WiFi – AP wewnętrzne	15
Łącznik światłowodowy	2

Lp.	Wymaganie	Spełnia TAK/ NIE
1.	**System klasy SIEM**	
1.1.	Rozwiązanie musi być systemem klasy SIEM / SOAR działającym w chmurze producenta z miejscem przechowywania logów na terenie UE.	
1.2.	Logowanie do instancji chmurowej rozwiązania, powinno umożliwiać wykorzystanie 2FA	
1.3.	Rozwiązanie musi umożliwiać przesyłania nieograniczonej ilości oraz wielkości logów, bez wpływu na konieczną do wykupienia licencję.	
1.4.	Rozwiązanie musi posiadać katalog minimum 140 gotowych integracji (przygotowane parsery) zdarzeń ze źródeł takich jak systemy, aplikacje i urządzenia bezpieczeństwa, ale także posiadać możliwość integracji źródeł z wykorzystaniem narzędzi wbudowanych do tworzenia paserów.	
1.5.	Rozwiązanie musi umożliwiać generowanie powiadomień o braku otrzymywania logów per pojedyncze źródło oraz zdefiniowany czas niedostępności logów.	
1.6.	Rozwiązanie musi posiadać możliwość dzielenia instancji głównej na pod instancje dla których mogą być zaimplementowane inne źródła logów oraz inne reguły bezpieczeństwa wyzwalające alerty w konsoli.	
1.7.	Rozwiązanie musi udostępniać możliwość instalacji przekaźnika logów instalowanego lokalnie na systemie Linux Debian i musi być to już gotowy kontener dostarczony przez producenta.	
1.8.	Rozwiązanie musi posiadać możliwość implementacji agenta na systemy Linux oraz Windows, który bezpośrednio będzie komunikował się z instancja chmurową oraz będzie monitorował system, na którym zostanie zainstalowany. Agent musi być dostępny w ramach licencji podstawowej.	
1.9.	Systemy, na których musi być możliwość instalacji agenta:	
	a) Windows 8	
	b) Windows 10	
	c) Windows 11	

	d) Windows Server 2016	
	e) Windows Server 2019	
	f) Windows Server 2022	
	g) Ubuntu 14.04 i nowszy	
	h) Debian 8 i nowszy	
	i) CentOS 7 i nowszy	
1.10.	W ramach integracji Agenta na systemie operacyjnym, minimum poniższe źródła danych oraz zdarzenia powinny być dostępne:	
	a) Access tokens	
	b) Authentication logs	
	c) DLL monitoring	
	d) File monitoring	
	e) Host network interface	
	f) Loaded DLLs	
	g) PowerShell logs	
	h) Process command-line parameters	
	i) Process monitoring	
	j) Process use of network	
	k) Windows event logs	
	l) Windows Registry	
1.11.	Rozwiązanie powinno mieć możliwość napisania własnych reguł na podstawie wzorca STIX lub SIGMA, wzorzec powinien być oparty na	

	formacie wartość. Rozwiązanie powinno także umożliwiać budowania reguł na podstawie zasilania informacjami CTI oraz na bazie anomalii	
1.12.	Rozwiązanie musi posiadać listę minimum 830 gotowych reguł bezpieczeństwa dostarczane przez producenta.	
1.13.	Katalog gotowych reguł musi być ciągle rozbudowywany przez producenta.	
1.14.	Rozwiązanie musi umożliwiać automatyczne powiadomienie o pojawieniu się nowej reguły przygotowanej przez producenta.	
1.15.	Implementacja nowych reguł bezpieczeństwa dostarczona przez producenta musi być możliwa w dwóch trybach:	
	a) w trybie automatycznym, gdzie nowa reguła jest automatycznie włączana do zestawu aktywnych reguł w momencie jej pojawienia się,	
	b) w trybie manualnym w którym administrator decyduje o jej włączeniu.	
1.16.	Rozwiązanie musi umożliwiać podział reguł na co najmniej 4 poziomy ze względu na ryzyko generowania przez nie fałszywych alarmów.	
1.17.	Uruchomione reguły muszą być wizualizowane w rozwiązaniu na bazie matrycy MITRE ATT&CK i pokrycia przez nie poszczególnych punktów w tej matrycy.	
1.18.	Rozwiązanie powinno umożliwiać wykorzystanie wskaźników naruszenia bezpieczeństwa (IoC) dostarczone przez producenta rozwiązania.	
1.19.	Rozwiązanie w karcie Alertu powinno wskazywać takie informacje jak:	
	a) typ alertu,	
	b) instancja, której dotyczy alert,	
	c) ważność alertu obliczane na bazie wagi (severity) reguły oraz krytyczności zasobu, którego dotyka alert,	
	d) typu detekcji (np. SIGMA),	
	e) informacje jakiego zasobu dotknął atak,	
	f) fazy ataku (w ramach Cyber Kill Chain),	

	g) treść wzorca reguły który wyzwolił alarm.	
1.20.	Rozwiązanie w panelu analityka musi umożliwiać podgląd listy zasobów (Assets) wykrywanych automatycznie przez system dzięki analizie zdarzeń oraz mapę ciepła aktywności zasobów na osi czasu.	
1.21.	Lista zasobów powinna zawierać minimum takie informacje jak:	
	a) nazwa,	
	b) typ zasobu,	
	c) ilość zdarzeń dotyczących danego zasobu,	
	d) ilość alertów dotyczących danego zasobu,	
	e) poziom Krytyczności zasobu.	
1.22.	Karta zasobu (Asset) powinna umożliwiać:	
	a) wpisanie tagu dla zasobu,	
	b) opisanie instancji do którego należy zasób,	
	c) manualne określenie krytyczności zasobu,	
	d) w przypadku użytkownika wpisanie maila,	
	e) w przypadku hosta wpisanie FQDN i dodatkowych adresów IP,	
	f) w przypadku hosta powinna umożliwić zmianę/opis typu systemu operacyjnego,	
	g) dodanie własnego opisu kontekstowego, odnoszącego się do zasobu np. numer seryjny urządzenia itp.	

1.23.	Rozwiązanie musi umożliwiać tworzenie playbooków w zakresie obsługi incydentów oraz delegowanie zadań do zdefiniowanych użytkowników.	
1.24.	Rozwiązanie musi umożliwiać przekazywanie notyfikacji z wykorzystaniem webhooks do Slack i Teams.	
1.25.	W ramach obsługi playbooków rozwiązanie powinno umożliwiać wewnątrz platformy stworzenie kont do systemów zewnętrznych z wykorzystaniem API w celu wzbogacania informacji ułatwiających analitykę. Platformy, które powinny być gotowe do integracji w rozwiązaniu to:	
	a) Binary Edge,	
	b) Virus Total,	
	c) Glimps,	
	d) Censys,	
	e) Shodan,	
	f) RiskIQ,	
	g) Iknowwhatyoudownload	
1.26.	Rozwiązanie w ramach playbooków powinno umożliwiać komunikacje z wykorzystaniem API do systemów zewnętrznych.	
1.27.	Rozwiązanie musi udostępniać modułu możliwy do instalacji w lokalnej infrastrukturze w celu wyzwalania zadań automatyzacji reagowania z poziomu sieci lokalnej w której znajdują się urządzenia, systemy docelowe.	
1.28.	System powinien być dostarczony z co najmniej 24 miesięcznym serwisem umożliwiającym korzystanie ze wsparcia producenta lub autoryzowanego serwisu producenta wraz z pobieraniem aktualizacji przygotowanych przez producenta. Jeśli standardowy okres wsparcia producenta lub dystrybutora jest dłuższy niż 24 miesiące lub Wykonawca wskazał w ofercie dłuższy okres, to okres wsparcia oprogramowania zostanie wydłużony odpowiednio o ten czas.	
2.	**System zarządzania dostępem uprzywilejowanym (PAM)**	

2.1.	System PAM musi być rozwiązaniem bezagentowym tj. umożliwiającym nawiązywanie sesji z wykorzystaniem serwerów proxy bez potrzeby instalacji oprogramowania (agenta) na systemie, do którego będzie nawiązywana sesja, umożliwiającym uwierzytelnianie wieloskładnikowe i obsługujące wiele platform i systemów operacyjnych. System PAM ma zabezpieczać dostęp do maszyn fizycznych, maszyn wirtualnych, sprzętu sieciowego m.in. routery, przełączniki, zapory sieciowe, aplikacje, bazy danych itp.	
2.2.	System musi być dostarczany w formie zamkniętej platformy wirtualnej przygotowanej do implementacji w infrastrukturze Hyper-V lub VMware. Przez zamkniętą platformę rozumiemy wyspecjalizowane rozwiązanie, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizująca wszystkie funkcjonalności systemu.	
2.3.	Rozwiązanie nie może wymagać wdrożenia kolejnych komponentów jako osobne maszyny wirtualne lub fizyczne. Do prawidłowego działania wszystkich dostępnych funkcjonalności wymagane jest posiadanie tylko jednej maszyny wirtualnej.	
2.4.	Rozwiązanie musi oferować wdrożenie drugiej instancji i konfiguracji klastra typu active-active.	
2.5.	System PAM musi zostać dostarczony z kompletem licencji dla co najmniej 5 użytkowników, którzy będą korzystali z Systemu PAM, minimum dla następującej liczby funkcjonalności:	
	a) Ochrona kont uprzywilejowanych,	
	b) Ochrona kluczy SSH,	
	c) Zarządzanie i monitorowanie sesji uprzywilejowanych,	
	d) Rejestrowanie sesji uprzywilejowanych	
	e) Raportowanie wykorzystania kont uprzywilejowanych,	
2.6.	Dostarczone licencje na System PAM do ochrony kont uprzywilejowanych nie mogą mieć ograniczeń czasowych. Dostarczone licencje będą udzielone bezterminowo.	
2.7.	Dostarczone licencje na system PAM nie mogą w żaden sposób limitować ilości chronionych systemów docelowych.	
2.8.	W ramach zakupionych licencji użytkownicy systemu muszą posiadać możliwość skorzystania z mechanizmu prywatnego sejfu.	

2.9.	System PAM musi zapewniać możliwość zarządzania (w szczególności):	
	a) Użytkownikami na systemach operacyjnych: Windows, Unix/Linux,	
	b) Kontami domenowymi: MS Active Directory,	
	c) Kontami lokalnymi: VMware ESX/ESXi,	
	d) Kontami na urządzeniach m.in.: Cisco, Aruba, Alcatel, CheckPoint, Fortigate, Huawei, IBM AIX, Brocade,	
	e) Kontami baz danych: Microsoft SQL, Oracle, MySQL, PostgreSQL	
	f) Kontami do zarządzania i monitorowania serwerów: m.in. iLO, iDRAC,	
	g) Kontami aplikacji webowych: Facebook, Google, Twitter, Linkedin, Instagram, Openstack, AWS	
	h) Kontami w innych niewymienionych systemach/urządzeniach do których dostęp odbywa się po protokołach: SSH, RDP, VNC, TELNET, HTTP/HTTPS,	
	i) Kluczami SSH.	
2.10.	System PAM musi umożliwiać utworzenie poświadczeń typu Just-in-Time (JIT), które będą tworzone lub aktywowane na czas trwania sesji.	
2.11.	System PAM musi umożliwiać usługę pośredniczenia w dostępie do systemów i urządzeń dla użytkowników domenowych oraz użytkowników zewnętrznych, rejestrując obsługiwane sesje, oraz obsługując minimum następujące protokoły: SSH, RDP, VNC, TELNET, HTTP/HTTPS, X11.	
2.12.	System PAM musi wspierać również protokoły bez rejestracji sesji: Cassandra, Elasticsearch, LDAP, LDAPS, MongoDB, MySQL, Oracle, PostgreSQL, Redis, Solr, SQL Server, RDS Sybase, Windows RM, Windows RPC, Windows SMB.	
2.13.	System PAM musi umożliwiać dostęp użytkowników do systemu docelowego następującymi narzędziami: przeglądarka internetowa,	
	a) klient RDP,	
	b) klient protokołu SSH/Telnet (np. putty),	

	c) klient serwerów bazodanowych m.in. DBeaver.	
2.14.	System PAM musi wspierać minimum następujące mechanizmy uwierzytelniania: LDAP, RADIUS, Tacacs Active Directory, OpenID, SAML.	
2.15.	System PAM musi zapewniać możliwość dwuskładnikowego uwierzytelniania.	
2.16.	System PAM musi wspierać integrację z rozwiązaniami dwuskładnikowego uwierzytelnienia takimi jak Google Authenticator i Microsoft Authenticator.	
2.17.	System PAM musi obsługiwać monitorowanie i ochronę kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego, do różnych systemów poprzez wiele lub jedno konto uprzywilejowane.	
2.18.	System PAM musi ograniczać administratorowi możliwość dostępu do haseł lub ograniczać podgląd do haseł uprzywilejowanych.	
2.19.	System PAM musi umożliwiać budowanie polityk kontroli dostępu w oparciu o role, np. na podstawie przynależności do grup AD/LDAP.	
2.20.	System PAM musi mieć możliwość zmiany wartości hasła na systemie docelowym zgodnie z ustawioną polityką m.in.:	
	a) umożliwiać zdefiniowanie wymagań na: długość hasła, znaki w haśle (małe i duże litery, cyfry, znaki specjalne),	
	b) generować automatycznie hasła kont systemów docelowych w sposób pseudolosowy,	
	c) generować unikalne hasła dla konta systemów docelowych,	
	d) wymuszać automatyczną zmianę hasła po jego podglądzie.	
2.21.	System PAM musi umożliwiać budowanie polityk kontroli dostępu wymuszającej:	
	a) podanie powodu rozpoczęcia sesji,	
	b) podanie powodu podglądu hasła,	
	c) konieczność akceptacji rozpoczęcia sesji przez innego administratora/ów,	
	d) konieczność akceptacji podglądu hasła przez innego administratora/ów,	

	e) zakresu godzin, dni oraz dat, kiedy użytkownik systemu będzie miał dostęp do poświadczeń.	
2.22.	System PAM musi umożliwiać udostępnienie poświadczenia do użytku dla użytkownika poza polityką dostępową, która jest do niego przypisana. Udostępnienie musi dawać możliwość wyboru długości trwania takiego dostępu.	
2.23.	System PAM musi posiadać log dla wszystkich zdarzeń systemowych.	
2.24.	System PAM musi umożliwiać wskazanie kont użytkowników, które realizowały logowanie do stacji/serwera.	
2.25.	System PAM musi umożliwiać raportowanie wszystkich zmian wprowadzonych przez administratorów.	
2.26.	System PAM musi umożliwiać raportowanie wszystkich logowań do systemu.	
2.27.	System PAM musi umożliwiać raportowanie oparte na nietypowym źródle, czasie i długości połączenia do systemu docelowego.	
2.28.	Rozwiązanie musi posiadać graficzną wizualizację przedstawiającą status bezpieczeństwa aktywnych oraz historycznych sesji do systemów zdalnych.	
2.29.	System PAM musi umożliwiać ograniczenie dostępu do raportów dla wskazanej grupy użytkowników lub administratorów.	
2.30.	System PAM musi umożliwiać transparentne połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego.	
2.31.	System PAM musi umożliwiać podgląd zestawionej sesji w czasie rzeczywistym.	
2.32.	System PAM musi umożliwiać przerwanie i/lub zawieszenie trwającej sesji.	
2.33.	System PAM musi posiadać menu pozwalające na zawieszenie lub przerwanie wszystkich sieci oraz zablokowanie dostępu do samego rozwiązania w przypadku sytuacji krytycznej.	
2.34.	System PAM musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie białych i czarnych list poleceń wykonywanych w systemie docelowym (audyt poleceń).	
2.35.	Audyt poleceń musi umożliwiać podjęcie co najmniej akcji, zablokuj polecenie i rozłącz sesję po wykryciu audytowanego polecenia a także automatyczne umieszczenie na liście blokowanych użytkowników użytkownika, który próbował wykonać blokowane polecenie.	

2.36.	Nagrywanie sesji nie może mieć żadnego wpływu na wydajność systemu docelowego.	
2.37.	System PAM musi umożliwiać konfigurację parametrów nagrań, w tym:	
	a) ilości klatek na sekundę,	
	b) jakości pojedynczej klatki,	
	c) formatu pojedynczej klatki: jpg lub png,	
	d) długości przechowywania nagrań.	
2.38.	System PAM musi rejestrować znaki wprowadzone z klawiatury przez użytkownika co najmniej dla sesji SSH i RDP oraz umożliwiać szybkie przeszukiwanie zapisanych danych pod kątem występowania wskazanych słów kluczowych.	
2.39.	System PAM musi umożliwiać utworzenie oddzielnego zestawu ustawień w oparciu o:	
	a) politykę dostępową,	
	b) urządzenie docelowe,	
	c) poświadczenie,	
	d) adresu źródłowego.	
2.40.	System PAM musi umożliwiać odtworzenie i pobranie zarejestrowanych nagrań sesji.	
2.41.	System PAM musi pozwalać na uruchomienie minimum następujących funkcjonalności:	
	a) zarządzać kontami uprzywilejowanymi w ramach organizacji,	
	b) monitorować wykorzystanie kont uprzywilejowanych,	
	c) nagrywać i archiwizować sesje zdalne,	
	d) gwarantować skalowalność rozwiązania w przypadku dodawania nowych zasobów oraz nowych usług,	

2.42.	System PAM musi umożliwiać personalizację wyglądu aplikacji co najmniej poprzez umieszczenie logo zamawiającego w głównym oknie aplikacji.	
2.43.	Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski.	
2.44.	System powinien być dostarczony z co najmniej 24 miesięcznym serwisem umożliwiającym korzystanie ze wsparcia producenta lub autoryzowanego serwisu producenta wraz z pobieranie aktualizacji przygotowanych przez producenta. Jeśli standardowy okres wsparcia producenta lub dystrybutora jest dłuższy niż 24 miesiące lub Wykonawca wskazał w ofercie dłuższy okres, to okres wsparcia oprogramowania zostanie wydłużony odpowiednio o ten czas.	
3.	**UTM – ochrona brzegu sieci**	
3.1.	System realizujący funkcję Firewall, zapewniający pracę w jednym z trzech trybów:	
	a) routera z funkcją NAT,	
	b) transparentnym,	
	c) monitorowania na porcie SPAN.	
3.2	System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.	
3.3.	System wspiera protokoły IPv4 oraz IPv6 w zakresie:	
	a) Firewall.	
	b) Ochrony w warstwie aplikacji.	
	c) Protokołów routingu dynamicznego.	
3.4	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS –możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.	

3.5.	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.	
3.6.	Monitoring stanu realizowanych połączeń VPN.	
3.7.	System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.	
3.8.	System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:	
	a) 18 portami Gigabit Ethernet RJ-45.	
	b) 4 gniazdami SFP+ 10 Gbps.	
	c) 4 gniazdami SFP28 10/25 GE.	
3.9.	System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.	
3.10.	System jest wyposażony w zasilanie 2x AC.	
3.11.	W zakresie Firewall'a obsługa nie mniej niż 7,5 mln. jednoczesnych połączeń oraz 500 tys. nowych połączeń na sekundę.	
3.12.	Przepustowość Stateful Firewall: nie mniej niż 135 Gbps dla pakietów 512 B.	
3.13.	Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 30 Gbps.	
3.14.	Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 14 Gbps.	
3.15.	W ramach systemu ochrony realizacja poniższych funkcji. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:	
	a) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.	
	b) Kontrola Aplikacji.	
	c) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.	

	d) Ochrona przed malware.	
	e) Ochrona przed atakami - Intrusion Prevention System.	
	f) Kontrola stron WWW.	
	g) Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.	
	h) Zarządzanie pasmem (QoS, Traffic shaping).	
	i) Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.	
	j) Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.	
	k) Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.	
	l) Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).	
3.16.	Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.	
3.17.	System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:	
	a) Translację jeden do jeden oraz jeden do wielu.	
	b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP.	
3.18.	W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.	

3.19.	Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.	
3.20.	Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.	
3.21.	Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.	
3.22.	Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.	
	a) Amazon Web Services (AWS).	
	b) Microsoft Azure.	
	c) Cisco ACI.	
	d) Google Cloud Platform (GCP).	
	e) OpenStack.	
	f) VMware NSX.	
	g) Kubernetes.	
3.23.	System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:	
	a) Wsparcie dla IKE v1 oraz v2.	
	b) Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).	
	c) Obsługa protokołu Diffie-Hellman grup 19, 20.	
	d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.	
	e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.	
	f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.	

	g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.	
	h) Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.	
	i) Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.	
	j) Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.	
	k) Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.	
	l) „Split tunneling" dla połączeń Client-to-Site.	
3.24.	System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:	
	a) Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.	
	b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.	
	c) Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.	
3.25.	W zakresie routingu rozwiązanie zapewnia obsługę:	
	a) Routingu statycznego.	
	b) Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).	
	c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.	
	d) Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.	

	e) ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.	
	f) BFD (Bidirectional Forwarding Detection).	
	g) Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.	
3.26.	System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.	
3.27.	SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).	
3.28.	System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.	
3.29.	System daje możliwość określania pasma dla poszczególnych aplikacji.	
3.30.	System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.	
3.31.	System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.	
3.32.	Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).	
3.33.	Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.	
3.34.	System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.	
3.35.	System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.	
3.36.	System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).	
3.37.	Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	

3.38.	System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.	
3.39.	System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	
3.40.	Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.	
3.41.	Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.	
3.42.	Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.	
3.43.	System chroni przed atakami na aplikacje pracujące na niestandardowych portach.	
3.44.	Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.	
3.45.	System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.	
3.46.	System dysponuje sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA.	
3.47.	Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).	
3.48	Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.	
3.49.	Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	
3.50.	Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.	
3.51.	Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.	

3.52.	Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.	
3.53.	Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.	
3.54.	Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).	
3.55.	System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).	
3.56.	Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.	
3.57.	W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.	
3.58.	Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.	
3.59.	Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.	
3.60.	Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).	
3.61.	Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.	
3.62.	Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.	
3.63.	Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.	
3.64.	System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.	
3.65.	System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:	

	a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.	
	b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.	
	c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.	
	d) System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.	
	e) System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.	
	f) Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.	
3.66.	Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.	
	a) Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.	
	b) Istnieje możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.	
	c) System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.	
	d) producent udostępnia dokumentację.	
	e) Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.	
	f) Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.	

	g) Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).	
	h) Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.	
3.67.	Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.	
3.68.	W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.	
3.69.	Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.	
3.70.	Możliwość włączenia logowania per reguła w polityce firewall.	
3.71.	System zapewnia możliwość logowania do serwera SYSLOG.	
3.72.	Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.	
3.73.	Urządzenie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski.	
3.74.	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane jest dostarczenie poniższych licencji:	
	a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Sygnatury ochrony systemów przemysłowych SCADA na okres 60 miesięcy.	
3.75.	Urządzenie musi być objęte serwisem gwarancyjnym producenta przez okres co najmniej 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Jeśli standardowy okres gwarancji producenta lub autoryzowanego serwisu producenta jest dłuższy niż 24 miesiące lub Wykonawca wskazał w ofercie dłuższy okres, to okres gwarancji zostanie wydłużony odpowiednio o ten czas.	

	W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, odbywa się bez dodatkowych kosztów po stronie Zamawiającego, realizowana przez producenta lub autoryzowanego dystrybutora w języku polskim przez okres wymaganej gwarancji.	
3.76.	System ma być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7 Wymagania powinny być potwierdzone dokumentami:	
	a) Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).	
	b) Certyfikat ISO 9001 podmiotu serwisującego.	
	c) Wymagane jest dostarczenie oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.	
4.	**Przełącznik agregacyjny 2 szt.**	
4.1.	Typ i liczba portów:	
	a) Minimum 48 portów 1/10-gigabitowych SFP+ umieszczonych z przodu obudowy;	
	b) Porty muszą wspierać wkładki działające co najmniej w standardach: 10GBaseSR, 10GBaseLR, 10GBaseT, 1000Base-T, 1000BaseSX, 1000BaseLX oraz kable DAC;	
	c) Minimum 4 porty 40/100GbE QSFP28 umieszczonych z przodu obudowy. Porty muszą wspierać co najmniej standardy: 100GBase-SR4, 100GBase-LR4, 100GBase-FR1, 40GBase-	

	SR4, 40GBase-eSR4, 40GBase-LR4, kable DAC i AOC oraz adaptery pozwalające na instalację wkładek 25Gb SFP28;	
	d) Wszystkie porty muszą być od siebie niezależne, nie dopuszcza się portów typu Combo;	
	e) Wbudowany, dodatkowy, dedykowany port Ethernet do zarządzania poza pasmem - out of band management;	
	f) Port konsoli RS232 ze złączem DB9 lub RJ45;	
	g) Port konsoli USB ze złączem USB-C;	
	h) Port USB 2.0 (niezależny od portu konsoli USB);	
4.2.	Wydajność: minimum 1,76 Tbps (prędkość przełączania „wirespeed" dla każdego portu przełącznika).	
4.3.	Przełączanie w warstwie 2 i 3 modelu OSI.	
4.4.	Wielkość bufora pakietów (packet buffer): minimum 32MB.	
4.5.	Modularny system operacyjny bazujący na jądrze Linux oraz wykorzystujący OVSDB.	
4.6.	Minimum 32GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash). Nie dopuszcza się pamięci instalowanej na zewnątrz przełącznika (np. do zewnętrznego portu USB)	
4.7.	Oprócz uruchamiania systemu operacyjnego Bootloader musi pozwalać na: dostęp do logów, zrzutów pamięci (coredump) i konfiguracji, naprawę i formatowanie przestrzeni pamięci, wgrywanie i aktualizację systemu operacyjnego, czyszczenie konfiguracji, czyszczenie i zmianę haseł administratorskich, wybór wersji systemu operacyjnego.	
4.8,	Minimum 16GB pamięci operacyjnej.	
4.9.	Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów).	
4.10.	Przepływ powietrza w przełączniku musi odbywać się w kierunku z przodu przełącznika do tyłu przełącznika. Nie dopuszczalne są rozwiązania, z mieszanym przepływem powietrza.	
4.11.	Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia.	

4.12.	Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)	
4.13.	Funkcja łączenia przełączników w grupy co najmniej 2 urządzeń, w sposób ciągły synchronizujących ze sobą konfiguracje przy zachowaniu niezależnych płaszczyzn zarządzani (control plane). Przełączniki połączone w grupę muszą zapewnić co najmniej: realizację łączy agregowanych w ramach różnych przełączników będących w grupie, architekturę, w której oba przełączniki są aktywne dla funkcji L2 i L3, funkcje typu ISSU lub Live Upgrade.	
4.14.	Tablica adresów MAC o wielkości minimum 140000 pozycji.	
4.15.	Obsługa ramek Jumbo o wielkości co najmniej 9kB.	
4.16.	Obsługa Quality of Service.	
4.17.	Obsługa mechanizmów, co najmniej: strict priority (SP) queuing, Deficit weighted round robin (DWRR) queuing oraz SP+DWRR.	
4.18.	Obsługa IEEE 802.1s Multiple SpanningTree (MSTP) oraz IEEE 802.1w Rapid Spanning Tree Protocol.	
4.19.	Obsługa sieci IEEE 802.1Q VLAN – minimum 1000 jednoczesnych sieci VLAN.	
4.20.	Obsługa IGMP v2/v3 (minimum 4000 grup), MLD (co najmniej 4000 grup), IGMP Snooping, PIM SM, PIM DM, PIM SSM.	
4.21.	Routing IPv4 – statyczny i dynamiczny (min. RIPv2, OSPF, BGP).	
4.22.	Routing IPv6 – statyczny i dynamiczny (min. RIPng, OSPFv3, MP-BGP).	
4.23.	Obsługa ECMP (Equal Cost Multi Path).	
4.24.	Obsługa VRRP.	
4.25.	Obsługa tunelowania GRE.	
4.26.	Obsługa Virtual Routing and Forwarding (VRF).	
4.27.	Obsługa funkcji VXLAN.	
4.28.	Tablica routingu o pojemności co najmniej 24000 wpisów dla IPv4, co najmniej 12000 wpisów dla IPv6.	

4.29.	Obsługa funkcji klienta DHCP.	
4.30.	Obsługa DHCP Relay dla IPv4 i IPv6.	
4.31.	Obsługa list ACL (co najmniej 16000) na bazie informacji z warstw 2 i 3 modelu OSI.	
4.32.	Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia.	
4.33.	Obsługa standardu 802.1p.	
4.34.	Funkcja ograniczania ruchu typu multicast i broadcast.	
4.35.	Możliwość zmiany wartości pola DSCP i/lub wartości priorytetu 802.1p.	
4.36.	Funkcja kopiowania ruchu wejściowego i wyjściowego (port mirroring) lokalnego (w obrębie urządzenia) i zdalnego (na porty znajdujące się na innym urządzeniu).	
4.37.	Funkcja centralnego uwierzytelniania administratorów na serwerze RADIUS oraz TACACS+.	
4.38.	Zarządzanie poprzez port konsoli (CLI), SNMP 2c, SNMP 3, interfejs graficzny (WebGUI) znajdujący się bezpośrednio na urządzaniu oraz SSH v2.	
4.39.	Obsługa Syslog.	
4.40.	Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP).	
4.41.	Obsługa sFlow.	
4.42.	Obsługa Network Time Protocol (NTP).	
4.43.	Obsługa Secure FTP (SFTP) oraz TFTP.	
4.44.	Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty.	

4.45.	Obsługa skryptów w języku Python.	
4.46.	Obsługa REST API.	
4.47.	Obsługa RMON (minimum grupy 1, 2, 3 i 9).	
4.48.	Obsługa funkcji diagnostycznych ping i traceroute dla IPv4 i IPv6.	
4.49.	Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego.	
4.50.	Przechowywanie co najmniej dwóch wersji oprogramowania na przełączniku.	
4.51.	Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).	
4.52.	Przełącznik musi posiadać mechanizm (automatycznego i ręcznego) tworzenia punktów szybkiego odtwarzania konfiguracji. Punkty szybkiego odtwarzania muszą zawierać aktualne zrzuty działającej konfiguracji oraz informacje dodatkowe (co najmniej: typ punktu, datę utworzenia, wersję oprogramowania, dane sprzętu, dane zapisującego punkt przywracania, opis). System musi umożliwiać ich kopiowanie i uruchamianie na innych urządzeniach tego samego typu. W urządzeniu musi być przechowywanych nie mniej niż 60 punktów przywracania konfiguracji. Przełącznik musi posiadać funkcję porównywania ze sobą (oraz prezentacji różnic) dwóch punktów odtwarzania konfiguracji oraz punktu odtwarzania konfiguracji z konfiguracją aktualnie działającą i konfiguracją zapisaną jako bieżąca.	
4.53.	Wysokość w szafie 19” – 1U o głębokości maksymalnie 45 cm.	
4.54.	Maksymalny pobór mocy nie większy niż 500W.	
4.55.	Minimalny zakres temperatur pracy od 0°C do 40°C.	
4.56.	Producent sprzętu musi być sklasyfikowany w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure” i znajdować się w kwadracie liderów (Leaders). Dane z najnowszego raportu aktualne na dzień ogłoszenia postępowania.	

4.57.	Wszystkie wymagane na przełączniku funkcje (o ile nie wyspecyfikowano inaczej) muszą być dostępne przez cały okres jego użytkowania (permanentne). Nie dopuszcza się licencji czasowych i subskrypcji.	
4.58.	Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania.	
4.59.	Przełącznik musi być w pełni obsługiwany (zarządzanie oraz monitoring) przez platformę chmurowego zarządzania kompatybilną z obecnie posiadanymi przez Zamawiającego przełącznikami HPE Aruba CX 6300 oraz CX 8100.	
4.60.	Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmuje wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu.	
4.61.	Przełącznik powinien być objęty dodatkowym wsparciem 24x7 w zakresie sprzętu, oprogramowania oraz dostępu do zespołów TAC (ang. technical assistance centers) na okres gwarancji wskazanej w ofercie - minimum 24 miesiące, a jeśli standardowy okres wsparcia producenta lub autoryzowanego serwisu producenta jest dłuższy niż 24 miesiące lub Wykonawca wskazał w ofercie dłuższy okres, to okres gwarancji zostanie wydłużony odpowiednio o ten czas.	
4.62.	Urządzenie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski.	
5.	**Przełącznik dostępowy 24 portowy**	
5.1.	Minimum 24 porty 100/1000BastT umieszczonych z przodu obudowy ze wsparciem dla standardu 802.3at (PoE+)	
5.2.	Minimum 4 porty 1/10-gigabitowe SFP+ umieszczone z przodu obudowy.	
5.3.	Przepustowość: minimum 127 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)	

5.4.	Wydajność: minimum 95 Mp/s.	
5.5.	Bufor pakietów: minimum 12 MB.	
5.6.	Minimum 4GB pamięci operacyjnej.	
5.7.	Minimum 16GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash).	
5.8.	Dedykowany port konsoli USB-C.	
5.9.	Port USB 2.0 (niezależny od portu konsoli USB).	
5.10.	Tablica adresów MAC o wielkości minimum 8000 pozycji.	
5.11.	Obsługa Jumbo Frames.	
5.12.	Obsługa sFlow lub Netflow.	
5.13.	Obsługa skryptów w języku Python.	
5.14.	Obsługa REST API.	
5.15.	Obsługa RMON (minimum grupy 1,2,3 i 9).	
5.16.	Obsługa 4094 tagów IEEE 802.1Q oraz 4094 jednoczesnych sieci VLAN.	
5.17.	Obsługa standardu 802.1v.	
5.18.	Obsługa protokołu MVRP.	
5.19.	Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne.	
5.20.	Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s).	
5.21.	Obsługa Secure FTP lub SCP.	

5.22.	Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP).	
5.23.	Obsługa SNTPv4 lub NTP.	
5.24.	Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping).	
5.25.	Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED).	
5.26.	Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting.	
5.27.	Obsługa uwierzytelniania użytkowników zgodna z 802.1x.	
5.28.	Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS.	
5.29.	Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW.	
5.30.	Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie.	
5.31.	Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+.	
5.32.	Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+.	
5.33.	Wbudowany serwer DHCP.	
5.34.	Obsługa funkcji User Datagram Protocol (UDP) helper.	
5.35.	Obsługa blokowania nieautoryzowanych serwerów DHCP.	
5.36.	Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego.	
5.37.	Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection).	

5.38.	Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP.	
5.39.	Zakres pracy od 0 do 45°C.	
5.40.	Zasilacz zapewniający budżet mocy PoE na poziomie nie niższym niż 370W.	
5.41.	Przełącznik w obudowie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 30 cm.	
5.42.	Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania.	
5.43.	Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.	
5.44.	Przełącznik musi być w pełni obsługiwany (zarządzanie oraz monitoring) przez platformę chmurowego zarządzania kompatybilną z obecnie posiadanymi przez Zamawiającego przełącznikami HPE Aruba CX 6300 oraz CX 8100.	
5.45.	Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmuje wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu.	
5.46.	Przełącznik powinien być objęty dodatkowym wsparciem 24x7 w zakresie sprzętu, oprogramowania oraz dostępu do zespołów TAC (ang. technical assistance centers) na okres gwarancji wskazanej w ofercie - minimum 24 miesiące, a jeśli standardowy okres wsparcia producenta lub autoryzowanego serwisu producenta jest dłuższy niż 24 miesiące lub Wykonawca wskazał w ofercie dłuższy okres, to okres gwarancji zostanie wydłużony odpowiednio o ten czas.	

5.47.	Urządzenie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski.	
6.	**Przełącznik dostępowy 48 portowy**	
6.1.	Minimum 48 porty 100/1000BastT umieszczonych z przodu obudowy ze wsparciem dla standardu 802.3at (PoE+)	
6.2.	Minimum 4 porty 1/10-gigabitowe SFP+ umieszczone z przodu obudowy.	
6.3.	Przepustowość: minimum 175 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)	
6.4.	Wydajność: minimum 98 Mp/s	
6.5.	Bufor pakietów: minimum 1 MB	
6.6.	Minimum 4GB pamięci operacyjnej	
6.7.	Minimum 16GB wewnętrznej pamięci nieulotnej typu Flash (eMMC, CF, SSD, SD, eUSB, SPI Flash).	
6.8.	Dedykowany port konsoli USB-C	
6.9.	Port USB 2.0 (niezależny od portu konsoli USB)	
6.10.	Tablica adresów MAC o wielkości minimum 8000 pozycji	
6.11.	Obsługa Jumbo Frames	
6.12.	Obsługa sFlow lub Netflow	
6.13.	Obsługa skryptów w języku Python	
6.14.	Obsługa REST API	
6.15.	Obsługa RMON (minimum grupy 1,2,3 i 9)	
6.16.	Obsługa 4094 tagów IEEE 802.1Q oraz 4094 jednoczesnych sieci VLAN	

6.17.	Obsługa standardu 802.1v	
6.18.	Obsługa protokołu MVRP	
6.19.	Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne	
6.20.	Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)	
6.21.	Obsługa Secure FTP lub SCP	
6.22.	Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)	
6.23.	Obsługa SNTPv4 lub NTP	
6.24.	Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)	
6.25.	Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)	
6.26.	Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting	
6.27.	Obsługa uwierzytelniania użytkowników zgodna z 802.1x	
6.28.	Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS	
6.29.	Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW	
6.30.	Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie	
6.31.	Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+	
6.32.	Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+	
6.33.	Wbudowany serwer DHCP	

6.34.	Obsługa funkcji User Datagram Protocol (UDP) helper	
6.35.	Obsługa blokowania nieautoryzowanych serwerów DHCP	
6.36.	Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego	
6.37.	Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)	
6.38.	Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP	
6.39.	Zakres pracy od 0 do 45°C	
6.40.	Zasilacz zapewniający budżet mocy PoE na poziomie nie niższym niż 370W	
6.41.	Przełącznik w obudowie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 33 cm.	
6.42.	Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania	
6.43.	Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.	
6.44.	Przełącznik musi być w pełni obsługiwany (zarządzanie oraz monitoring) przez platformę chmurowego zarządzania kompatybilną z obecnie posiadanymi przez Zamawiającego przełącznikami HPE Aruba CX 6300 oraz CX 8100.	
6.45.	Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmuje wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony	

	bezpośrednio przez producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu.	
6.46.	Przełącznik powinien być objęty dodatkowym wsparciem 24x7 w zakresie sprzętu, oprogramowania oraz dostępu do zespołów TAC (ang. technical assistance centers) na okres gwarancji wskazanej w ofercie - minimum 24 miesiące, a jeśli standardowy okres wsparcia producenta lub autoryzowanego serwisu producenta jest dłuższy niż 24 miesiące lub Wykonawca wskazał w ofercie dłuższy okres, to okres gwarancji zostanie wydłużony odpowiednio o ten czas.	
6.47.	Urządzenie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski.	
7.	**Wkładki SFP+**	
7.1.	Typ interfejsu: SFP+	
7.2.	Typ wkładki: single-mode	
7.3.	Złącze światłowodowe: LC	
7.4.	Maksymalny dystans transferu: 10 km	
7.5.	Długość fali TX: 1310 nm	
7.6.	Długość fali RX: 1310 nm	
7.7.	Wkładki w pełni kompatybilne z oferowanymi przełącznikami z pkt. 4, 5, 6. Montaż i używanie wkładek z w/w przełącznikami nie może powodować utraty gwarancji producenta oferowanych przełączników.	
8.	**System zarządzania przełącznikami i Access Pointami**	
8.1.	System musi być zbudowany w architekturze klient – serwer	
8.2.	Dostęp do sytemu zarządzania musi być realizowany przez przeglądarkę internetową	
8.3.	System musi być zbudowany modułowo, tak aby możliwe było doinstalowanie modułu dającego dodatkową funkcjonalność	

8.4.	System zarządzania musi spełniać podstawowe funkcje:	
	a) Automatyczne wykrywanie topologii sieci	
	b) Monitorowanie stanu urządzeń po protokole SNMP	
	c) Konfiguracja urządzeń po protokole SNMP	
	d) Konfiguracja list dostępu (ACL) na zarządzanych urządzeniach	
	e) Konfiguracja VLANów na zarządzanych urządzeniach	
	f) Zarządzenie konfiguracją urządzeń, tworzenie backupów oraz grupowe implementowanie konfiguracji przechowywanych w systemie zarządzania	
	g) Zarządzenie zdarzeniami, przypisywanie alarmów do różnego rodzaju zdarzeń	
	h) Możliwość wysyłania alarmów np. mailem lub SMS'em	
	i) Generowanie raportów w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta	
	j) Obrazowanie sieci w postaci mapki wraz z wyróżnianiem kolorami występujących alarmów	
	k) Lokalizowanie użytkowników po adresie IP lub MAC	
	l) Możliwość utworzenia mapki sieciowej obrazującej połączenia sieciowe związane z zarejestrowanym atakiem sieciowym	
8.5.	Muszą być dostępne moduły umożliwiające rozbudowę i integrację systemu o następujące funkcjonalności:	
	a) Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA	
	b) Obługa informacji przesyłanych z wykorzystaniem sFlow oraz Netstream z urządzeń sieciowych oraz obrazowanie wyników	
	c) Zarządzenie systemem telefonii IP	

	d) Zarządzenie sieciami sieciami MPLS oraz sieciami VPN w oparciu o MPLS oraz VPLS	
	e) Moduł do monitorowania stanu/zdrowia usług	
8.6.	Niezbędne jest aby system zarządzania był w stanie podłączyć się i importować dane z Active Directory	
8.7.	System musi mieć możliwość automatycznego tworzenia i rozsyłania raportów	
8.8.	Wymagana jest możliwość tworzenia kont administratorskich z różnymi poziomami uprawnień, z możliwością przypisywania administratorów do grup urządzeń	
8.9.	Oferowane rozwiązanie musi obejmować licencjami 500 urządzeń sieciowych od różnych producentów.	
8.10.	Dla wszystkich obsługiwanych standardowo urządzeń musi być dostępnie nie tylko monitorowanie, ale również zarządzanie, czyli możliwość modyfikacji konfiguracji urządzeń.	
8.11.	Musi również mieć możliwość implementacji rozproszonej, wykorzystując różne serwery do instalacji swoich komponentów.	
8.12.	Oprogramowanie do zarządzania siecią musi pochodzić od tego samego producenta jak oferowane przełączniki. Nie dopuszcza się rozwiązań mieszanych, od wielu dostawców z wieloma punktami kontaktu w razie awarii.	
8.13.	System powinien być dostarczony z co najmniej 24 miesięcznym serwisem umożliwiającym korzystanie ze wsparcia producenta lub autoryzowanego serwisu producenta wraz z pobieranie aktualizacji przygotowanych przez producenta. Jeśli standardowy okres wsparcia producenta jest dłuższy niż 24 miesiące lub Wykonawca wskazał w ofercie dłuższy okres, to okres wsparcia oprogramowania zostanie wydłużony odpowiednio o ten czas. Wsparcie powinno być świadczone w trybie 24x7.	
8.14.	Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski.	
9.	**System NAC, autoryzowany dostęp do sieci w warstwie fizycznej, sieciowej i aplikacyjnej oraz 802.1X.**	

9.1.	System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor).	
9.2.	System musi odsługiwać minimum 2500 urządzeń klienckich (w tym gości). Licencje mają dotyczyć aktualnie podłączonych urządzeń i mają być zwalniane po rozłączeniu urządzenia.	
9.3.	Praca jako maszyna wirtualna.	
9.4.	Musi posiadać wbudowany serwer Radius oraz TACACS +.	
9.5.	Musi wspierać RADIUS VSA co najmniej 100 producentów, w tym:	
	a) Cisco Systems	
	b) Fortinet	
	c) Microsoft	
	d) Alcatel-lucent Enterprise	
	e) HPE Aruba Networks	
	f) Huawei	
	g) Extreme Networks	
	h) PaloAlto	
9.6.	System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera.	
9.7.	System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego.	
9.8.	Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.	

9.9.	Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych	
	a) Microsoft Active Directory	
	b) Radius	
	c) Kerberos	
	d) LDAP	
	e) ODBC	
	f) Współpraca z serwerami tokenów	
9.10.	Musi obsługiwać metody profilowania	
	a) DHCP	
	b) TCP	
	c) MAC OUI	
	d) SNMP	
	e) Cisco device sensor	
9.11.	Wspierać protokoły	
	a) Radius, Radius CoA, TACACS +, web authentication, SAML v2.0	
	b) EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)	
	c) PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD)	
	d) TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)	
	e) EAP-TLS	

	f) PAP, CHAP, MSCHAPv1 i v2, EAP-MD5	
	g) NAC, Microsoft NAP	
	h) Windows machine authentication	
	i) MAC Auth	
	j) Audit (role oparte na porcie oraz skanowanie podatności)	
	k) OCSP (Online Certificate Status Protocol)	
	l) SNMP generic MIB, SNMP private MIB	
	m) CEF (Common Event Format), LEEF (Log Event Extended Format)	
	n) TLS 1.2	
9.12.	Funkcja integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami.	
9.13.	Maszyna wirtualna musi mieć możliwość uruchomienia na platformach witalizacyjnych:	
	a) Co najmniej ESX 4.0, ESXi 4.1 do 6.0	
	b) Co najmniej Hyper-V 2012 R2 oraz Windows 2012 R2 enterprise	
9.14.	Posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (2500). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte. System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności:	
	a) Samodzielna rejestracja klientów gościnnych w oparciu o:	
	I. Adres e-mail	
	II. Numer telefonu (wiadomość SMS)	

	III. Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link)	
	b) Logowanie w oparciu o portale społecznościowe	
	c) Funkcja integracji z systemami trzecimi poprzez API	
	d) Wsparcie dla tworzenia komercyjnych systemów HOT-SPOT wykorzystujących do płatności systemy płatności karta kredytową	
	e) Wbudowany system reklamowy umożliwiający integrację z zewnętrznymi serwisami umożliwiającymi w prosty sposób promowanie ofert promocyjnych, materiałów multimedialnych oraz aplikacji mobilnych.	
	f) Wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych.	
	g) Funkcja personalizacji strony gościnnej	
9.15.	Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.	
	a) Konfiguracja urządzeń ma odbywać się bez potrzeby angażowania pracowników działo IT	
	b) System musi wspierać obsługę następujących systemów operacyjnych	
	I. MS Windows	
	II. Mac OS X	
	III. iOS	
	IV. Android	
	V. Chromebook	

	VI. Ubuntu	
	c) Umożliwienie klientowi samo rejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci	
	d) Automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej	
	e) Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu.	
	f) Funkcja tworzenia unikalnych certyfikatów dla urządzeń.	
	g) Wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń	
	h) Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID	
9.16.	Posiadać moduł odpowiedzialny za kontrolę końcówek klienckich. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji. System kontroli końcówek klienckich musi mieć następujące funkcjonalności:	
	a) System musi wspierać następujące systemy operacyjne	
	I. Microsoft Windows 7 i nowsze (może być uruchomiony jako serwis)	
	II. Apple	
	III. Red HAT Enterprise Linux 4 i nowsze	
	IV. CentOS 4 (Community Enterprise Operating System) i nowsze	
	V. Fedora Core 5 i nowsze	
	VI. SUSE linux 10.x i nowsze	
	b) Funkcja kontroli stanu oprogramowania anty-wirusowego, anty-spyware, firewall	

	c) Wyświetlanie informacji on-line o statusie monitorowanych końcówek	
	d) System powinien obsługiwać agenta w formie	
	I. Stałej (Presistent Agent)	
	II. Tymczasowej (Dissolvabe Agent)	
	III. Agenta NAP	
9.17.	System powinien być dostarczony z co najmniej 24 miesięcznym serwisem umożliwiającym korzystanie ze wsparcia producenta lub autoryzowanego serwisu producenta wraz z pobieranie aktualizacji przygotowanych przez producenta. Jeśli standardowy okres wsparcia producenta jest dłuższy niż 24 miesiące lub Wykonawca wskazał w ofercie dłuższy okres, to okres wsparcia oprogramowania zostanie wydłużony odpowiednio o ten czas. Wsparcie powinno być świadczone w trybie 24x7. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.	
9.18.	Do rozwiązania musi być dostępna publicznie, na stronie producenta, dokumentacja techniczna opisująca wdrożenie i użytkowanie systemu. Wszystkie wymagane funkcje muszą być dostępne w chwili składania oferty i udokumentowane (opisane w dokumentacji lub możliwe do sprawdzenia na wersji ewaluacyjnej systemu) (nie dopuszcza się scenariusza, w którym jakieś elementy są zaplanowane do realizacji w przyszłości). Zamawiający zastrzega sobie prawo do weryfikacji spełnienia wymagań.	
9.19.	Zamawiający może zażądać przed dostawą przeprowadzenia testów wybranych funkcji sprzętu i oprogramowania wymaganych w niemniejszym postępowaniu. Testy potwierdzające działania wymaganych funkcji muszą zostać przeprowadzone w siedzibie Zamawiającego w terminie nie dłużysz niż 2 tygodnie od chwili zażądania przez Zamawiającego ich przeprowadzenia. Nieprzystąpienie do testów lub nieskuteczne ich przeprowadzenie (brak potwierdzenia przez Zamawiającego, że testy zostały zakończone pomyślnie) skutkować będzie odrzuceniem oferty.	

9.20.	Oprogramowanie NAC musi pochodzić od tego samego producenta jak oferowane przełączniki. Nie dopuszcza się rozwiązań mieszanych, od wielu dostawców z wieloma punktami kontaktu w razie awarii.	
9.21.	Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski.	
10.	**Radiowy punkt dostępowy wewnętrzny**	
10.1.	Minimalne wymagania punktu dostępowego działającego wewnątrz budynku:	
	a) technologia radiowa 5GHz 2x2:2 oraz 2,4GHz 2x2:2	
	b) tryb radiowy – SSR (antena wybierana programowo):	
	• 2,4GHz / 5GHz	
	• 5GHz / 5GHz – Dual 5GHz	
	• Czujnik (2,4GHz / 5GHz) / 5GHz	
	c) praca w środowisku o wysokim zagęszczeniu użytkowników	
	d) obsługa WPA3 zapewniająca najnowszy standard bezpieczeństwa użytkownikom i urządzeniom IoT	
	e) filtr CCF minimalizujący wpływ z sieci komórkowych	
	f) standard zasilania 802.af oraz 802.at przy korzystaniu z portu USB	
	g) zarządzanie urządzeniami w chmurze lub przez kontroler sprzętowy/wirtualny	
10.2.	Szczegółowe parametry punktu dostępowego wewnętrznego:	
	a) SSID na radio / łącznie: 8/16	
	b) Max. ilość użytkowników na radio / łącznie: 512/1024	

c) standard 802.11n	
• zakres częstotliwości 2,4-2,5GHz i 5,150-5,850GHz	
• modulacja 802.11n	
• prędkości (Mb/s): MCS0-MCS15 (6,5 Mb/s – 300 Mb/s)	
• radio 2x2:2 MIMO	
• obsługa HT20 dla 2,4GHz i 5GHz	
• obsługa HT40 dla 5GHz	
• agregacja ramek A-MPDU i A-MSDU	
d) standard 802.11ac	
• zakres częstotliwości 5,150-5,850GHz	
• modulacja 802.11ac (256QAM)	
• prędkości (Mb/s): MCS0-MCS9 (6,5 Mb/s – 867 Mb/s), NSS = 1-2	
• radio 2x2:2 MIMO	
• kanał 20MHz	
• VHT20/VHT40/VHT80 wsparcie	
• formowanie wiązki TxBF Beamforming	
e) standard 802.11ax	
• zakres częstotliwości 2,4-2,5GHz i 5,150-5,850GHz	
• modulacja 802.11ax (1024QAM)	

• OFDMA dla łącza w górę i dół	
• prędkości dla 5GHz (Mbps): HE0-HE11 (8 Mbps – 1200 Mbps)	
• prędkości dla 2,4GHz (Mbps): HE0-HE11 (8 Mbps – 574 Mbps)	
• radio 2x2:2 MIMO	
• obsługa HE20/HE40/HE80 dla 5 GHz	
• obsługa HE20/HE40 dla 2,4 GHz	
• odbieranie i wysyłanie wielu strumieni danych: DL SU-MIMO i MU-MIMO	
• formowanie wiązki TxBF Beamforming	
f) standard IoT	
• BLE Zgodność ze standardami Bluetooth® Low Energy (BLE) i IEEE® 802.15.41	
g) interfejsy	
• 2 porty Ethernet 10/100/1000 z automatycznym wykrywaniem, RJ45	
• port USB 3.0 typu A, 0,5A	
h) zasilanie	
• standard PoE IEEE 802.3af	
i) pobór mocy	
• standardowo 9W i max: 11,1 W bez USB	
• standardowo 12W i max: 14 W z USB	

	j) anteny	
	• dla jednostki ze zintegrowanymi antenami: antena dookólna dla 2,4GHz/5GHz, antena dookólna dla 5GHz oraz antena dookólna dla BLE w zakresie 2,4-2,5GHz	
	• dla jednostki wyposażonej w złącza antenowe zewnętrzne: złącza RP-SMA zarówno dla częstotliwości 2,4GHz, 5GHz i BLE	
	k) bezpieczeństwo	
	• obsługa najnowszych certyfikatów bezpieczeństwa Wi-Fi Alliance WPA3 oraz obsługa zapory sieciowej L2-L7 DPI	
	l) odporność na wyładowania	
	• kontaktowe +/- 8kV	
	• powietrzne +/- 15kV	
11.	**Radiowy punk dostępowy zewnętrzny**	
11.1.	Minimalne wymagania punktu dostępowego działającego zewnętrznego:	
	a) technologia 3-radiowa 5GHz 4x4:4 oraz 2,4GHz 2x2:2, 2,4GHz/5GHz/Czujnik	
	b) tryb radiowy – SSR (antena wybierana programowo):	
	• 2,4GHz / 5GHz / Czujnik (2,4GHz/5GHz)	
	• 5GHz / 5GHz – Dual 5GHz	
	c) praca w środowisku o wysokim zagęszczeniu użytkowników	
	d) obsługa WPA3 zapewniająca najnowszy standard bezpieczeństwa użytkownikom i urządzeniom IoT	
	e) filtr CCF minimalizujący wpływ z sieci komórkowych	

	f) standard zasilania 802.at	
	g) zarządzanie urządzeniami w chmurze lub przez kontroler sprzętowy/wirtualny	
	h) praca w zakresie temperatur od -40 do + 60°C	
11.2.	Szczegółowe parametry punktu dostępowego zewnętrznego:	
	a) SSID na radio / łącznie: 8/16	
	b) Max. ilość użytkowników na radio / łącznie: 512/1024	
	c) standard 802.11n	
	• zakres częstotliwości 2,4-2,5GHz i 5,150-5,850GHz	
	• modulacja 802.11n	
	• prędkości (Mb/s): MCS0-MCS31 (6,5 Mb/s – 600 Mb/s)	
	• radio 2x2:2 MIMO	
	• obsługa HT20 dla 2,4GHz i 5GHz	
	• obsługa HT40 dla 5GHz	
	• agregacja ramek A-MPDU i A-MSDU	
	d) standard 802.11ac	
	• zakres częstotliwości 5,150-5,850GHz	
	• modulacja 802.11ac (256QAM)	
	• prędkości (Mb/s): MCS0-MCS9 (6,5 Mb/s – 3467 Mb/s), NSS = 1-4	
	• radio 2x2:2 MIMO	

• kanał 20MHz	
• obsługa VHT20/VHT40/VHT80	
• formowanie wiązki TxBF Beamforming	
e) standard 802.11ax (dla czujnika 5GHz)	
• zakres częstotliwości 5,150-5,850GHz	
• modulacja 802.11ax (1024QAM)	
• OFDMA dla łącza w górę i dół	
• prędkości (Mbps): HE0-HE11 (8 Mbps – 1200 Mbps), NSS = 1-2	
• radio 2x2:2 MIMO	
• obsługa VHT20/VHT40/VHT80/VHT160	
• formowanie wiązki TxBF Beamforming	
f) standard 802.11ax (dla radia 5GHz)	
• zakres częstotliwości 2,4-2,5GHz i 5,150-5,850GHz	
• modulacja 802.11ax (1024QAM)	
• OFDMA dla łącza w górę i dół	
• prędkości dla 5GHz (Mbps): HE0-HE11 (8 Mbps – 4800 Mbps)	
• prędkości dla 2,4GHz (Mbps): HE0-HE11 (8 Mbps – 574 Mbps)	
• radio 4x4:4 MIMO	
• obsługa VHT20/VHT40/VHT80/VHT160 dla 5GHz	

• obsługa VHT20/VHT40 dla 2,4GHz	
• formowanie wiązki TxBF Beamforming	
g) standard IoT	
• BLE Zgodność ze standardami Bluetooth® Low Energy (BLE)	
h) interfejsy	
• porty Ethernet 100/1000/2500 Mb/s z automatycznym wykrywaniem, RJ45, port PoE zasilanie 802.3at	
• porty Ethernet 10/100/1000 Mb/s z automatycznym wykrywaniem, RJ45,	
• port USB 2.0 typu A, 5V, 0,5A	
i) zasilanie	
• standard PoE IEEE 802.3af	
j) pobór mocy	
• standardowo 21,7W i max: 25,3 W bez USB	
• standardowo 18,2W i max: 20,8 W z USB	
k) anteny	
• dla jednostki ze zintegrowanymi antenami: antena dookólna dla 2,4GHz/5GHz, antena dookólna dla 5GHz oraz antena dookólna dla BLE w zakresie 2,4-2,5GHz lub anteny sektorowe (60° lub 120°) w zależności od potrzeby pokrycia terenu – różne wersje zewnętrznej jednostki AP	
l) bezpieczeństwo	

	• obsługa najnowszych certyfikatów bezpieczeństwa Wi-Fi Alliance WPA3 oraz obsługa zapory sieciowej L2-L7 DPI	
	m) odporność na wyładowania	
	• kontaktowe +/- 8kV	
	• powietrzne +/- 15kV	
	n) obudowa o stopniu ochrony IP67	

*Przez dni robocze należy rozumieć wszystkie dni tygodnia oprócz sobót, niedziel i innych dni ustawowo wolnych od pracy w Polsce.

Załącznik nr 4 – Opis przedmiotu zamówienia

Sposób realizacji projektu

1. Projekt będzie realizowany w 3 zadaniach, obejmujących prace związane z zaprojektowaniem, dostawą i wdrożeniem poszczególnych elementów projektu:

   Zadanie 1
   1) Dostawa wraz z instalacją przełącznika agregacyjnego, przełączników dostępowych 24 i 48 portowych, wkładek SFP.
   2) System/y zarządzania przełącznikami i Access Pointami (Network Management System).
   3) Autoryzacja 802.1X w sieci LAN.
   4) System NAC, autoryzowany dostęp do sieci w warstwie fizycznej, sieciowej i aplikacyjnej.
   5) Zarządzanie dostępem uprzywilejowanym (PAM).
   6) UTM w celu ochrony brzegu sieci OT.

   Zadanie 2
   1) Rozbudowa sieci WiFi.

   Zadanie 3
   1) Przełącznik przemysłowy 8 portowy.
   2) UTM w celu ochrony brzegu sieci OT.
   3) System SIEM.

2. W ramach każdego z zadań Wykonawca będzie zobowiązany do zrealizowania wszystkich czynności niezbędnych do prawidłowego wdrożenia zakresu prac danego zadania, wskazanych w ustępie 1 oraz związanego z tym zakresem:

   a. Opracowanie projektu technicznego; projekt podlega akceptacji Zamawiającego.

   b. Opracowania dokumentacji powykonawczej,

   c. Instruktaży i szkoleń autoryzowanych,

   d. Testów funkcjonalnych (o ile są wymagane).

3. Wdrożenie i uruchomienie dostarczonych produktów odbędą się w miejscu wskazanym przez Zamawiającego i we współpracy z Zamawiającym, wraz z wykonaniem niezbędnych połączeń sieciowych – połączenie serwerowni podstawowej i zapasowej. Projekt takiego połączenia musi być uwzględniony.

4. Wykonawca będzie zobowiązany do przedstawienia w ciągu 14 dni od popisania umowy szczegółowego planu prac (harmonogram), z uwzględnieniem powyższych zadań, obejmujących realizację prac dla poszczególnych produktów, opisanych w dalszej części. Plan zostanie opracowany w uzgodnieniu z Zamawiającym oraz zatwierdzony przez Zamawiającego, jako podstawa do dalszych prac.

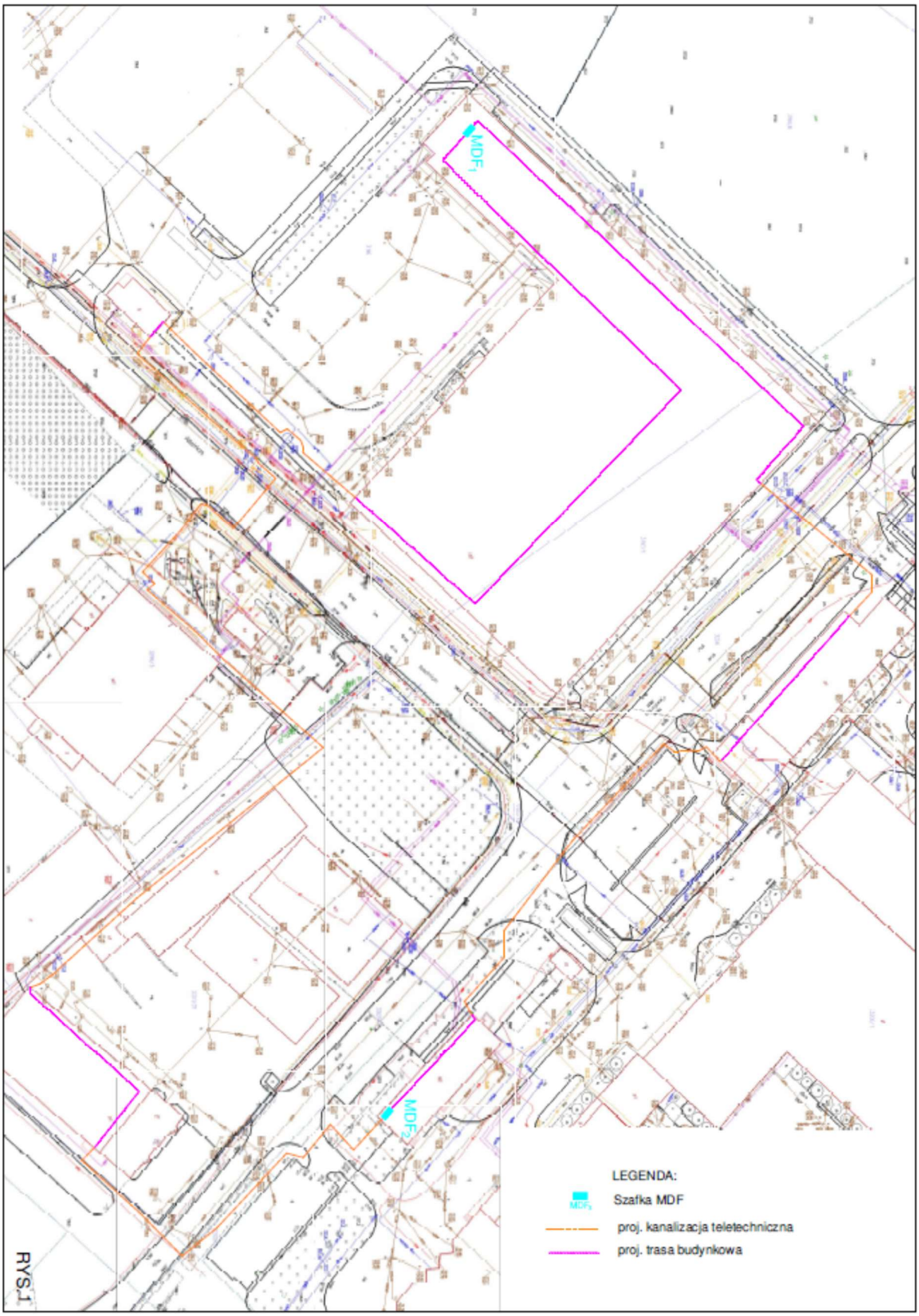
5. Plan prac, wskazany w pkt. 4, powinien obejmować wszystkie produkty projektu, realizowane w ramach danego zadania, wskazane z ustępie 1.

6. Wykonawca, w toku realizacji prac, będzie działać w porozumieniu z Zamawiającym, uzgadniając wszelkie szczegółowe terminy prac, szczególnie związanych ze zmianami sieć IT i OT, co najmniej na 3 dni robocze przed przystąpieniem do nich.
7. Projekt techniczny powinien obejmować wszystkie elementy niezbędne do prawidłowego montażu/instalacji i konfiguracji poszczególnych produktów oraz wykonania prac instalacyjnych, w tym:
    a. analizę infrastruktury teleinformatycznej Zamawiającego związanej z realizacją Umowy,
    b. uzgodnienie konfiguracji bazującej na wymaganiach polityki bezpieczeństwa Zamawiającego,
    c. stworzenie koncepcji implementacji polityk bezpieczeństwa w oparciu o analizę aktualnie działającego środowiska,
    d. zebranie informacji o wykorzystywanych rodzajach urządzeń końcowych,
    e. uzgodnienie schematu sieci w zakresie niezbędnym do wdrożenia urządzeń lub oprogramowania,
    f. stworzenie mapowania ról użytkowników oprogramowania,
    g. plan integracji z systemem domenowym,
    h. uzgodnienie polityk dostępu.
8. W zakresie szkoleń Wykonawca zobowiązany będzie do zapewnienia:
    a. autoryzowanych przez producenta szkoleń ze wszystkich dostarczonych produktów sieciowych (nie dotyczy sieci WiFi), zakończonych wydaniem certyfikatu odbycia szkolenia,
    b. szkoleń z zakresu cyberbezpieczeństwa sieci przemysłowych, trwające minimum 3 dni szkoleniowe.
2. Szkolenia mogą być dostarczone w formie voucherów, ważnych co najmniej 1 rok lub wykupione w trakcie realizacji projektu. W takim wypadku terminy odbycia szkoleń zostaną ustalone z Zamawiającym z co najmniej 14 dniowym wyprzedzeniem.
3. Wykonawca, w toku realizacji poszczególnych zadań przeprowadzi Instruktaże dla co najmniej 2 administratorów z zakresu konfiguracji wdrożonych urządzeń sieciowych, sieci WiFi, połączenia światłowodowego oraz wdrożonego oprogramowania SIEM, PAM i zarządzania siecią. Instruktaże powinny trwa co najmniej 2 godziny robocze na każdy zakres prac, w trybie stacjonarnym, w terminach ustalonych z Zamawiającym.

Łącznik światłowodowy pomiędzy serwerowniami

1. Przedmiotem prac jest zaprojektowanie i wybudowanie dwóch niezależnych połączeń światłowodowego pomiędzy serwerowniami wraz z zakończeniem na przełącznicach modułowych.
2. Oba łączniki światłowodowe należy wybudować z wykorzystaniem istniejącej kanalizacji kablowej i traktów kablowych w budynkach. W przypadku niedrożności lub braku ciągłości kanalizacji należy ją udrożnić lub wybudować jej nowe fragmenty.

3. Mapa przebiegu istniejących tras kablowych przedstawiono na rys nr 1.



4. W budynkach kable należy prowadzić istniejącymi traktami i korytami kablowymi, w przypadku braku miejsca lub zmian tras należy uwzględnić budowę dodatkowych koryt i tras kablowych.

Zakres prac projektowych

1. W ramach zamówienia jest wykonanie kompletnej dokumentacji projektowej umożliwiającej wykonanie szkieletowej instalacji telekomunikacyjnej w oparciu o technologię światłowodową pomiędzy wskazanymi lokalizacjami.
2. Dokumentacja powinna zawierać zakresy projektu budowlanego w przypadku kanalizacji kablowej oraz zakresy wykonawcze i technologiczne w przypadku instalacji kabla światłowodowego w budynkach wraz z jego zakończeniem na przełącznicach światłowodowych.
3. Urządzenia, technologie i materiały powinny być opisane i scharakteryzowane w jednoznaczny i wyczerpujący sposób.
4. W celu wykonania dokumentacji projektowej należy przeprowadzić inwentaryzacje istniejącej Infrastruktury Zamawiającego, zweryfikować drożność i zajętość kanalizacji kablowej.
5. Dokumentacja projektowa powinna zostać wykonana zgodnie z obowiązującymi przepisami, opublikowanymi normami, zasadami najlepszej wiedzy technicznej oraz z zachowaniem zasady należytej staranności Wykonawcy.
6. Po zakończeniu prac budowlanych należy sporządzić dokumentacją powykonawczą budowlaną, zinwentaryzować geodezyjnie nowe fragmenty kanalizacji oraz wykonać aktualizację powykonawcza dokumentacji wykonawczej. Do opracowania należy dołączyć dokumentacje pomiarową wykonaną zgodnie z wymaganiami opisanymi poniżej.

Dostawy i roboty budowlane

1. Prace budowlane i instalacyjne należy rozpocząć po opracowaniu i zatwierdzeniu przez Zamawiającego dokumentacji projektowej budowlanej i projektu wykonawczego.
2. W ramach zadania należy sprawdzić drożności oraz ewentualnie udrożnić kanalizacji pomiędzy studniami kablowymi na zaprojektowanej trasie przebiegu linii światłowodowej.
3. Wykonanie przepustów kablowych do budynków oraz zastosowanie zabezpieczeń gazoszczelnych i wodoszczelnych.
4. Montaż linii kablowej światłowodowej w istniejącej lub zmodernizowanej kanalizacji telekomunikacyjnej w relacjach budynek biurowy serwerownia podstawowa MDF1 – część biurowa budynku produkcyjnego dz. Nr.3196 MDF2 dwiema niezależnymi trasami.
5. Montaż kabli światłowodowych w budynkach w istniejących korytach i traktach kablowych.
6. Montaż zapasów kabli, wchodzących do budynków, w obudowach naściennych.
7. Wybudowanie w razie potrzeb i zgodnie z dokumentacja techniczną wykonawczą dodatkowych fragmentów tras kablowych w budynkach i na konstrukcjach.

8. Wprowadzenie kabli do pomieszczeń serwerowni podstawowej i rezerwowej.
9. Zakończenie kabli światłowodowych na przełącznicach światłowodowych w szafach teleinformatycznych.
10. Oznakowanie kabli światłowodowych na całej trasie przebiegu w studniach, przy przepustach, przy wejściach do budynku oraz przy przełącznicach.
11. Zakończenie wszystkich włókien kabli światłowodowych na dostarczonych przełącznicach.
12. Dostawa oraz montaż czterechprzełącznic optycznych modułowych o parametrach:
    a) ilość portów 48x SM SC/APC
    b) wymiar – 2U 19”
    c) w pełni wysuwalna obudowa na prowadnicach
    d) zabezpieczenie dochodzących patchcordów, poprzez zastosowanie półek osłonowy
    e) możliwość podwojenia pojemności przełącznicy przez zastosowanie łączników LC duplex
13. Należy dostarczyć akcesoria instalowane dodatkowo w szafie: organizery patchcordów, organizer tub oraz wieszaki na patchcordy.
14. Kolejność spawania włókien zgodna z normą IEC 60304 lub IEC 304 lub OTO (ZN-11/TP S.A-005-2) do uzgodnienia z Zamawiającym na etapie realizacji zgodnie z dokumentacją wykonawczą.
15. Dostawa patchcordów łączeniowych:
    a) SM SC/APC – SC/APC SIMPLEX o długości 1m – 12 szt.
    b) SM SC/APC – SC/APC SIMPLEX o długości 3m – 12 szt.
    c) LC/UPC-SC/APC SIMPLEX o długości 3m – 12 szt.
    d) LC/UPC-SC/APC DUPLEX o długości 3m – 12 szt.
16. Dla wybudowanych linii światłowodowych należy wykonać pomiary według poniższych wytycznych.
17. Wytyczne w zakresie pomiarów linii światłowodowych:
    f) Pomiar tłumienności wynikowej torów metodą transmisyjną, dla każdego włókna światłowodowego w obu oknach optycznych w obu kierunkach
    g) Pomiary właściwości teletransmisyjnych torów światłowodów metodą reflektometryczną, na wszystkich włóknach dla fali 1310nm i 1550nm z obu stron odcinka, pomiędzy przełącznicami optycznymi.
    h) Pomiary reflektometryczne na zmontowanej linii powinny umożliwić określenie:

- całkowitej długości optycznej linii;

- całkowitej tłumienności linii oraz tłumienności połączeń

i) Tłumienność jednostkowa każdego włókna toru światłowodowego (bez połączeń) nie może przekraczać wartości określonej przez producenta dla kabli danej klasy, wybranych przez projektanta w sposób umożliwiający spełnienie wymagań bilansu mocy

j) Maksymalna tłumienność dla złącz spawanych nie może przekroczyć 0,1 dB w obu kierunkach transmisji. Maksymalna tłumienność dla złącz rozłącznych nie może przekroczyć 0,5 dB w obu kierunkach transmisji. Wyniki pomiarów wraz z wykresami reflektancji i tabelami zdarzeń dla całych torów optycznych dla danej relacji, należy załączyć do dokumentacji powykonawczej w formie dokumentu utworzonego bezpośrednio z urządzenia pomiarowego.

18. Podstawowe parametry dla zastosowanego kabla światłowodowego:

d) jednomodowy, włókno G.652D (SM) 9/125 µm

e) minimalna ilość włókien 48J

f) ilość tub 4 lub 8

g) odporny na promieniowanie UV

h) w kanalizacji kablowej zewnętrznej należy stosować kabel o wzmocnionej powłoce, odporny na gryzonie

i) kabel układany wewnątrz budynków biurowych powinien być w wykonaniu bezhalogenowym nierozprzestrzeniające płomienia (LSOH)

19. Zastosowany kabel światłowodowy jednodomowy powinien umożliwiać transmisję na poziomie minimum 100 Gb/s.

Rozbudowa sieci WiFi

1. Zamawiający posiada system Wi-Fi znajdujący się na terenie zakładu w Grajewie przy ul. Elewatorskiej 13, nie obejmuje on jednak zasięgiem całego terenu zakładu.
2. Zamawiający na terenie Zakładu posiada infrastrukturę sieciową która podlegać będzie modernizacji i uzupełnieniu o przyłącza niezbędne do uruchomienia sieci Wi-Fi;
3. Istniejący zespół nadajników radiowych AP nadzorowany jest za pośrednictwem centralnego systemu zarządzania, który zaimplementowany jest na urządzeniach Zamawiającego.
4. Zamawiający posiada zainstalowaną następującą infrastrukturę sprzętową oraz licencje:

LP	Nazwa	PN	Szt.
1	Access Point wewnętrzny	AP310i-WR	6
	Access Point wewnętrzny	AP410C-WR	2
	Access Point wewnętrzny	AP410i-WR	5
	Access Point wewnętrzny	AP5010-WW	1

	Access Point wewnętrzny	AP-7632-680B30-WR	20
2	Access Point zewnętrzny	AP460C-WR	83
	Access Point zewnętrzny	AP460S12C-WR	23
	Access Point zewnętrzny	AP-7662-680B40-WR	45
3	Kontroler wirtualny WLAN	WiNG VX9000 (klaster)	2
4	Licencje	VX9000-1	208
5	Licencje	VX9000-A74B12	64

5. Przedmiotem zamówienia jest zaprojektowanie, dostawa i wdrożenie kompletnego systemu Wi-Fi na terenie zakładu w Grajewie, który umożliwi pokrycie zasięgiem obszaru całego Zakładu.
6. Zamówienie dotyczy dostawy i wdrożenia punktów dostępowych wewnętrznych i zewnętrznych dokładna liczba poszczególnych urządzeń wynikać będzie przeprowadzonej inwentaryzacji i planowania radiowego.
7. Przedmiot zamówienia obejmuje realizacje następujących czynności:
   a) Wykonanie inwentaryzacji istniejącego systemu Wi-Fi i infrastruktury sieciowej na potrzeby dostarczanego systemu Wi-Fi;
   b) Wykonanie fizycznych pomiarów terenowych i planowania radiowego uwzględniającego aktualne warunki terenowe, uzgodnienie z Zamawiającym miejsca lokalizacji punktów dostępowych;
   c) Wykonanie projektu technicznego wykonawczego spełniającego wymagania określone poniżej;
   d) Instalację i uruchomienie urządzeń składających się na system Wi-Fi spełniający wymagania Zamawiającego określone w dalszej części OPZ;
   e) Wybudowanie połączeń kablowych i elementów zasilania umożliwiających uruchomienie i przyłączenie punktów dostępowych do sieci Zamawiającego;
   f) Modernizacje i integrację elementów infrastruktury technicznej zamawiającego pod kątem instalacji systemu Wi-Fi;
   g) Konfigurację dostarczonego sprzętu oraz zainstalowanych urządzeń systemu Wi-Fi i integracja z istniejącym systemu Wi-Fi w jedna strukturę;
   h) Wykonanie konfiguracji, uruchomienia i wdrożenia Systemu Wi-Fi pokrywającej obszar Zakładu zgodnie z zatwierdzoną dokumentacja wykonawczą, ustawienie kanałów radiowych, mocy wypromieniowanej przez poszczególne access points, ustawienia parametrów sieciowych;

i) Przeprowadzenie testów akceptacyjnych dla dostarczonych i zainstalowanych i urządzeń, zgodnie z opracowanym planem testów akceptacyjnych;

j) Do każdego punktu dostępowego powinny być dostarczone niezbędne licencje umożliwiające ich prace w deklarowanym okresie oraz licencje pozwalająca na zarządzanie nim w klastrze kontrolerów Zamawiającego.

k) Dostarczone urządzenia muszą być zarejestrowane na koncie Zamawiającego w portalu pomocy technicznej producenta posiadać wsparcie w zakresie pomocy technicznej producenta oraz aktualizacji oprogramowania przez okres gwarancji i wsparcia.

l) Opracowanie kompleksowej dokumentacji powykonawczej;

Wymagania w zakresie Projektu Technicznego sieci WiFi

1. Wykonawca opracuje i dostarczy Zamawiającemu Projekty techniczne sieci WiFi. Przed przystąpieniem do wykonania projektu technicznego Wykonawca zobowiązany jest wykonać wizję lokalną na terenie Zakładu. Termin wizji lokalnej musi zostać uzgodniony z przedstawicielem Zamawiającego.
2. Zamawiający wymaga dostarczania przez Wykonawcę Projektu Technicznego składającego się z minimum następujących elementów:
   1) Dokumentacja techniczna rozmieszczenia punktów dostępowych i plan radiowy wraz z rozkładem propagacji radiowej uwzględniający pokrycie zasięgiem w pasmach 2,4GHz oraz 5,0 GHz podanych przez Zamawiającego obszarów Zakładu zawierający:
      a) Siłę sygnału dla wszystkich punktów dostępowych;
      b) Lokalizację punktów dostępowych;
      c) Rozkład kanałów radiowych;
      d) SNR (signal-to-noise ratio);
      e) Przepustowość sieci;
      f) Nakładanie kanałów (channel overlap)
      g) Przybliżoną lokalizację aktualnie zainstalowanych AP z wyszczególnieniem dla każdego z parametrów: SSID, BSSID, Kanał nadawania
   2) Dokumentacja techniczną wykonawczą zawierająca m.in.
      a) przebiegi kablowe;
      b) miejsce instalacji AP, detale konstrukcyjne;
      c) topologia fizyczna infrastruktury;
      d) rozmieszczenie urządzeń w istniejących węzłach sieciowych i szafach;
      e) schematy elektryczne i podłączenie urządzeń do istniejących obwodów elektrycznych;
      f) schematy logiczne i adresację urządzeń sieciowych;

g) zestawienia ilościowe urządzeń i elementów systemu.

3) Dokumentacja powykonawcza zawierająca elementy wymienione w punkcie 1 i 2 zaktualizowane o zmiany wynikłe w trakcie wdrożenia systemu oraz dodatkowo:

a) dokumentacje sprawdzeń i pomiarów wybudowanych połączeń sieciowy;

b) dokumentacje pomiarową radiową obrazująca osiągnięcie zadanych parametrów;

c) protokoły sprawdzeń i pomiarów elektrycznych.

Wymagania w zakresie wdrożenia systemu Wi-Fi

1. Zamawiający wymaga instalacji sprzętu (access point) na istniejących elementach stałych tj. budynki i konstrukcje dostosowując sposób instalacji do lokalnych warunków.
2. Przewody sygnałowe i zasilające prowadzić należy istniejącymi traktami kablowymi, w przypadku ich braku należy przewidzieć budowę drabin i koryt kablowych, przewody prowadzić w osłonach „peszlach".
3. Dostarczone urządzenia radiowe należy połączyć z istniejącym kontrolerem sieci bezprzewodowej oraz istniejącymi punktami dostępowymi (AP) za pośrednictwem istniejących linii sygnałowych i infrastruktury pasywnej.
4. Wykonawca musi dostarczyć okablowanie sygnałowe miedziane lub światłowodowe niezbędne do połączenia nowo dostarczonych urządzeń z istniejącą infrastrukturą sieciową Zamawiającego.
5. Wykonawca musi dostarczyć wkładki światłowodowe niezbędne do podłączenia urządzeń do istniejącej infrastruktury sieciowej, jeżeli wystąpi potrzeba ich zastosowania.
6. Zamawiający wymaga, aby dostarczone urządzenia sieciowe zostały uruchomione w infrastrukturze logicznej umożliwiając funkcjonowanie z istniejącymi punktami dostępowymi i istniejącym lokalnym kontrolerem sieci bezprzewodowej.
7. Należy przewidzieć dostawę dodatkowych licencji umożliwiających prace dostarczanych punktów Wi-Fi a w przypadku zmiany rozwiązania dostaw kompletnego systemu centralnego kontrolera wraz z licencjami.
8. Prace wdrożeniowe będą prowadzone bez wstrzymania ruchu i pracy Zakładu w całym okresie realizacji Umowy wraz z okresem gwarancyjnym;
9. Prace będą prowadzone w terminie ustalonym z Zamawiającym. Zamawiający przewiduje, że część prac będzie prowadzona poza godzinami pracy poszczególnych części Zakładu.
10. Należy przewidzieć dostawę dodatkowych licencji umożliwiających prace dostarczanych punktów Wi-Fi a w przypadku zmiany rozwiązania dostaw kompletnego systemu z centralnym kontrolerem i kompletem licencji.

Podstawowe wymagania w zakresie osiągnięcia założonych parametrów sieci Wi-Fi

1. Zamawiający wymaga pokrycia zasięgiem oddziaływania sieci Wi-Fi całego terenu Zakładu.

2. Transfer danych w standardach 802.11a/g, oraz transfer danych w standardzie 802.11n, ac, ax, w tym także możliwość przesyłania ruchu głosowego.
3. Roaming połączeń między AP.
4. Siła sygnału AP powinna być ustawiona zgodnie z regulacjami prawnymi obowiązującymi w tym zakresie w RP, tj. zgodnie z normą ETSI maksymalnie 100mW dla pasma 2,4GHz oraz 200mW dla pasma 5,0GHz, z pozostawieniem marginesu na zwiększenie mocy w przypadku awarii sąsiednich AP.
5. W celu umożliwienia działania z wysokimi prędkościami przyjąć siłę sygnału na granicy zasięgu komórki RSSI – 70 dBm;
6. Pomiary sieci bezprzewodowej i mapy zasięgu mają zostać przygotowane w dedykowanym oprogramowaniu osobno dla częstotliwości 2,4Ghz oraz 5Ghz.
7. Rzeczywiste mapy pomiarów, potwierdzające osiągnięcie planowanych parametrów radiowych, mają zawierać w szczególności:
   a) Siłę sygnału dla wszystkich punktów dostępowych
   b) Siłę sygnału pojedynczych punktów dostępowych
   c) Rozkład kanałów radiowych
   d) SNR (signal-to-noise ratio)
   e) Przepustowość sieci
   f) Nakładanie kanałów (channel overlap)

Wymagania w zakresie integracji elementów infrastruktury technicznej systemu Wi-Fi z systemem zarządzania Zamawiającego

1. Zamawiający wymaga przeprowadzenia Integracji uruchomionej Infrastruktury Wi-Fi z istniejącym systemem zarządzania opartym o kontroler WLAN ExtremeWireless VX900 pracującego w klastrze 2x WiNG VX 9000 Exream.
2. W zakresie użytkowym Zamawiający wymaga pełnej integracji zamawianego sprzętu sieciowego z systemem zarządzania wymienionym w punkcie 1 powyżej w następujących obszarach funkcjonalnych:
   a) wdrożenia urządzeń do użytkowania w infrastrukturze zamawiającego (onboarding) – uproszczone uruchamianie i konfigurację;
   b) zarządzania licencjami z poziomu komponentów VX;
   c) zdalnej konfiguracji;
   d) monitoringu na poziomie globalnym, lokalnym i klienta;
   e) diagnostyki;
   f) raportowania;

3. Integracja jest niezbędna w celu grupowania i jednolitego zarządzania wszystkich urządzeń wchodzących w skład sieci Wi-Fi w Zakładzie Zamawiającego w ZMP Grajewo ale również pozostałych Zakładach Spółdzielni.

Gwarancja

1. Gwarancja obejmuje wyłącznie wady powstałe z przyczyn tkwiących w dostarczonych lub wytworzonych w ramach realizacji Umowy produktach, tj. w urządzeniach, oprogramowania, konfiguracji, instalacji lub dokumentacji.
2. Okres gwarancji na dostarczone oprogramowanie oraz na dostarczony sprzęt komputerowy, będzie liczony w okresie odpowiadającym co najmniej 24 miesiącom od daty podpisania bez zastrzeżeń protokołu odbioru danego sprzętu, w ramach poszczególnych zadań projektu. Jeśli standardowy okres wsparcia producenta jest dłuższy niż 24 miesiące lub Wykonawca wskazał w ofercie dłuższy okres gwarancji, to okres wsparcia zostanie wydłużony odpowiednio o ten czas.
3. Gwarancja obejmuje prawidłowe działanie systemu i sprzętu, zgodnie z opisanymi w OPZ parametrami i wymaganiami funkcjonalnymi oraz przekazaną przez Wykonawcę dokumentacją techniczną.
4. Wykonawca zapewni dla wszystkich urządzeń gwarancję producenta lub autoryzowanego serwisu producenta. Udzielona gwarancja nie może być gorsza niż standardowe warunki producenta lub autoryzowanego serwisu producenta dla danego
5. Wykonawca zobowiązany jest do nieodpłatnego usuwania błędów z przyczyn zawinionych przez Wykonawcę, będących konsekwencją wystąpienia: błędu w dokumentacji administratora lub powykonawczej, błędu w wykonaniu usług wdrożenia przez Wykonawcę.
6. Błędy i awarie w okresie gwarancji i w zakresie prac wykonanych przez Wykonawcę, w tym w dokumentacji lub konfiguracji oprogramowania w celu zapewnienia rozliczalności będą zgłaszane Wykonawcy za pomocą elektronicznej platformy zgłoszeń. Wykonawca zapewni platformę zgłoszeń bezpłatnie.
7. Wykonawca zapewni przyjmowanie zgłoszeń gwarancyjnych przez system zgłoszeń gwarancyjnych przez całą dobę przez wszystkie dni w roku w trybie 24/7/365.
8. Usunięcie błędów oznacza przekazanie przez Wykonawcę do Zgłaszającego, nowej wersji oprogramowania lub poprawki lub rekonfiguracji oprogramowania lub urządzenia lub też poprawki dokumentacji oraz usunięcie skutków błędu.
9. System zgłoszeń powinien umożliwiać Zamawiającemu pobieranie raportów zawierających takie informacje jak wykaz wszystkich zgłoszeń wraz z identyfikatorem zgłoszenia, wskazanie ewentualnego modułu / komponentu w systemie, którego dotyczy Zgłoszenie, priorytet zgłoszenia, dane osoby zgłaszającej, sposób rozwiązania zgłoszenia, treść odpowiedzi w przypadku zapytania, opis modyfikacji w przypadku modyfikacji, datę i godzinę rejestracji, datę i godzinę zamknięcia zgłoszenia.

Dodatkowe wymagania w zakresie serwisu powdrożeniowego i świadczeń gwarancyjnych sieci WiFi

1. Wykonawca zobowiązuje się w ramach świadczeń gwarancyjnych przedmiotu zamówienia:
   a) Zamawiający wymaga, aby Gwarancja w zakresie dostarczonego Sprzętu obejmowała diagnozowanie i usuwanie przez Wykonawcę wszystkich usterek dostarczonego sprzętu;
   b) W razie konieczności, w terminie zgodnym z zapisami Umowy, wymianę i dostarczenie sprzętu nowego, wolnego od wad, spełniającego wymagania jak dla sprzętu zastępowanego. Uszkodzone/zużyte części i podzespoły wymontowane ze sprzętu stają się własnością Wykonawcy, natomiast części dostarczone przez Wykonawcę z chwilą ich wymiany przechodzą na własność Zamawiającego. Zamawiający potwierdzi wymianę Sprzętu Protokołem odbioru ilościowego Sprzętu w ramach wymiany.
   c) wymiana części i podzespołów nie może spowodować zwiększenia kosztów eksploatacji, obsługi, potencjalnej rozbudowy i utylizacji naprawianego Sprzętu;
   d) Wykonawca w ramach gwarancji będzie zobowiązany do świadczenia Administratorom Zamawiającego wsparcia, w szczególności:
      1) rozwiązywania problemów dotyczących bieżącej eksploatacji i konfiguracji Urządzeń Systemu Wi-Fi,
      2) zapewnienia aktualizacji systemu i firmware urządzeń wchodzących w jego skład wraz z instrukcją instalacji (o ile jest niezbędna),
      3) uczestnictwa w procesie aktualizacji, implementacji polityk bezpieczeństwa Zamawiającego.
   e) Wykonawca będzie zobowiązany na okres trwania gwarancji do zapewnienia co najmniej jednego dedykowanego opiekuna Inżyniera, wskazanego w wykazie osób, załączonego do Oferty Wykonawcy, do koordynacji, co najmniej w zakresie:
      1) obsługi zgłoszeń gwarancyjnych,
      2) obsługi wsparcia technicznego,
      3) komunikacji pomiędzy Wykonawcą, a Zamawiającym.
   f) Wsparcie, o którym mowa w pkt e), będzie świadczone w dni robocze, w godz. 8.00-16.00. Zamawiający przewiduje limit godzin wsparcia na 24 godzin w ciągu roku.
2. Zapewnienie serwisu powdrożeniowego, który obejmuje:
   a) w przypadku wystąpienia awarii urządzenia, Wykonawca zobowiązany jest do usunięcia awarii i świadczenia serwisu na zasadach opisanych poniżej:
   b) Wykonawca zagwarantuje zapewnienie dwóch kategorii SLA:
      1) Kategoria 1 – wymagane parametry SLA w zakresie czasów usuwania awarii pojedynczych punktów dostępowych, maksymalnie 5 punktów - podjęcie działań serwisowych, reakcja w czasie 4 godzin od zgłoszenia, podjęcie działań

serwisowych w miejscu instalacji mających na celu wyeliminowanie awarii w czasie do 24 godzin od zgłoszenia,

2) Kategoria 2 – SLA w zakresie czasów usuwania awarii powyżej 5 punktów dostępowych lub kontrolera sieci i elementów zarządzania - podjęcie działań serwisowych, reakcja w czasie 2 godzin od zgłoszenia, podjęcie działań serwisowych w miejscu instalacji mających na celu wyeliminowanie awarii w czasie do 12 godzin od zgłoszenia.

c) Usługi SLA, o których mowa powyżej będą świadczone dla Kategorii 2 - 24 godziny na dobę, a dla Kategorii 1 w dni robocze od poniedziałku do piątku w godzinach 8:00 – 16:00;

d) Dopuszczalny łączny czas niedostępności systemu Wi-Fi w ciągu roku kalendarzowego nie może przekroczyć 128 h w przypadku sumy godzin dla pojedynczego access point i 64 h dla systemu zarządzania i nadzoru.

e) Serwis urządzeń musi być świadczony w miejscu użytkowania urządzeń.

f) Dopuszcza się możliwość naprawy w serwisie Wykonawcy, jeśli naprawa w lokalizacji użytkownika okaże się niemożliwa. W takim przypadku wymagane jest dostarczenie urządzenia zastępczego o nie gorszych parametrach, w terminach zgodnych z SLA jak wyżej.

g) Wykonawca zobowiązany będzie przeprowadzić przeglądy prewencyjne całego Systemu Wi-Fi w każdym roku świadczenia serwisu w odstępach 12 miesięcznych.

h) Przegląd prewencyjny będzie polegał na:

i. sprawdzeniu poprawności działania systemu,

ii. analizie plików komunikatów o błędach,

iii. sprawdzeniu i ew. korekcie (po akceptacji Zamawiającego) wersji oprogramowania,

iv. zmiany konfiguracyjne na wniosek Zamawiającego,

v. inne prace wymagane przez producenta rozwiązania.

i) Rekonfigurację systemu na wniosek i według potrzeb Zamawiającego

Odbiory prac

1. Procedura dotyczy odbiorów dokonywanych w ramach realizacji Projektu, określonych w harmonogramie wdrożenia projektu, w tym również Odbioru końcowego projektu.

Odbiór zadania

1. Odbiory zadań dokonywane są w terminach wskazanych w Harmonogramie wdrożenia Projektu.
2. W ramach odbioru zadania, dokonuje się weryfikacji ilościowej, kompletności dostarczenia lub wytworzenia wszystkich produktów projektu, zgodnie z założeniami określonymi w harmonogramie wdrożenia.

3. W ramach Odbioru zadania zostaną przeprowadzone odpowiednie testy funkcjonalne, opisane w pkt. Procedura testowania
4. Wykonawca przystępując do odbioru zadania musi przedstawić Zamawiającemu:
    1) Potwierdzenie przeprowadzenia testów funkcjonalnych, przyjęty przez Zamawiającego bez zastrzeżeń.
    2) Komplet dokumentacji dotyczącej każdego produktu, dostarczanego w ramach zadania.
    3) W przypadku produktu dotyczącego Infrastruktury sprzętowej - karty katalogowe dla każdego urządzenia.
    4) Gwarancje lub poświadczenia uruchomienia serwisów producenta na produkty wykonane i dostarczone w trakcie trwania odbieranego produktu. Zamawiający, na wniosek Wykonawcy, może wyrazić zgodę na uruchomienie serwisów producenta w późniejszym terminie, ale nie później niż przed podpisaniem protokołu odbioru końcowego.
5. Odbiór zadania potwierdzony jest Protokołem odbioru podpisanym przez Wykonawcę i Zamawiającego bez zastrzeżeń. Jeżeli protokół odbioru zadania będzie zawierał zastrzeżenia, zadanie uważa się za nieodebrane.
6. Dokonanie odbioru zadania, nie pozbawia Zamawiającego roszczenia wobec Wykonawcy o usunięcie wad, które ujawnią się w odebranych już Komponentach, w trakcie realizacji kolejnych zadań przedmiotu Umowy, a także w okresie gwarancji.
7. Protokół odbioru zadania, zostanie sporządzony w dwóch jednobrzmiących egzemplarzach - dla Zamawiającego i dla Wykonawcy.
8. W ramach odbioru zadania, jeżeli jest to zaplanowane w harmonogramie, zostaną przeprowadzone odpowiednie testy funkcjonalne, opisane w pkt. Procedura testowania
9. Wykonawca przystępując do odbioru zadania musi przedstawić:
    1) Raport z przeprowadzonych testów funkcjonalnych, przyjęty przez Zamawiającego bez zastrzeżeń (jeżeli były wykonywane w ramach odbioru zadania),
    2) Niezbędne licencje na produkty wykonane i dostarczone w trakcie trwania odbieranego zadania.
10. Dokonanie odbioru zadania, nie pozbawia Zamawiającego roszczenia wobec Wykonawcy o usunięcie wad, które ujawnią się w odebranych już produktach wykonanych i dostarczonych w ramach zadania, w trakcie realizacji kolejnych zdań przedmiotu Umowy, a także w okresie gwarancji.
11. Wady produktów wykonanych i dostarczonych w ramach konkretnego zadania, zdiagnozowane w późniejszych zadaniach, zostaną niezwłocznie (jednak nie później niż w terminie wskazanym w warunkach gwarancji poszczególnych produktów) usunięte przez Wykonawcę bez odrębnego wynagrodzenia. Zamawiający nie przewiduje, w związku z opisanymi w zadaniach poprzednich okolicznościami, zmiany terminów wykonywania przedmiotu Umowy, w tym kolejnych zadań.

Odbiór końcowy

1. Odbiór końcowy odbędzie się w terminie wskazanym w harmonogramie wdrożenia projektu.
2. W ramach odbioru końcowego dokonuje się weryfikacji ilościowej, czy zostały odebrane wszystkie zadania, zgodnie z założeniami określonymi w harmonogramie wdrożenia projektu.
3. Wykonawca przystępując do Odbioru końcowego musi przedstawić:
   1) Wszystkie protokoły odbioru zadań wymagane w ramach odbioru końcowego,
   2) Potwierdzenie usunięcia wszystkich wad ujawnionych po odbiorach produktów i odbiorach zadań.
4. Odbiór końcowy potwierdzony jest protokołem odbioru końcowego podpisanym przez Wykonawcę i Zamawiającego bez zastrzeżeń. Protokół zostanie sporządzony w dwóch jednobrzmiących egzemplarzach - dla Zamawiającego i dla Wykonawcy.
5. Jeżeli Protokół odbioru końcowego będzie zawierał istotne zastrzeżenia, projekt uważa się za nieodebrany.

Procedura testowania

1. Procedura dotyczy testów funkcjonalnych produktów poprzedzających odbiór zadania, zgodnie z planem projektu. Termin i czas przeprowadzenia poszczególnych testów funkcjonalnych zostanie określony w planie projektu.
2. Zakres testów funkcjonalnych, będzie odpowiadał zakresowi realizacji prac w ramach wykonania lub dostarczenia danego produktu w ramach danego zadania i musi obejmować co najmniej:
   1) kompletność, poprawność instalacji i działania oprogramowania,
   2) kompletność, poprawność instalacji i działania Infrastruktury sprzętowej i infrastruktury sieciowej,
3. Iteracje testów i reakcja na wady w trakcie wykonywania testów funkcjonalnych:
   1) Pierwsza iteracja testów:
      a) w trakcie testów Zamawiający na bieżąco zgłasza Wady.
      b) po zakończeniu realizacji całego scenariusza testowego, Wykonawca przekaże Zamawiającemu protokół rozbieżności, zawierający Wady.
      c) czas usunięcia wszystkich Wad po pierwszej iteracji: do 5 dni roboczych od przekazania protokołu rozbieżności.
   2) Druga iteracja testów – weryfikacja usuniętych wad zgłoszonych w pierwszej iteracji testów:
      a) w trakcie testów Zamawiający na bieżąco zgłasza Wady.

b) po zakończeniu realizacji testów, Wykonawca przekaże Zamawiającemu protokół rozbieżności, zawierający Wady.

c) czas usunięcia wszystkich Wad po drugiej iteracji: do 3 dni roboczych od przekazania protokołu rozbieżności.

3) Trzecia iteracja testów – weryfikacja usuniętych Wad zgłoszonych w poprzednich iteracjach testów:

a) w trakcie testów Zamawiający na bieżąco zgłasza Wady.

b) po zakończeniu realizacji całego scenariusza testowego, Wykonawca przekaże Zamawiającemu protokół rozbieżności, zawierający Wady.

c) czas usunięcia wszystkich Wad po trzeciej iteracji: do 2 dni roboczych od przekazania protokołu rozbieżności.

4) Czwarta iteracja testów – weryfikacja usuniętych Wad zgłoszonych w poprzednich iteracjach testów.

4. W sytuacji, gdy pomimo dokonania wszystkich iteracji testów wskazanych, testy nie zakończą się pomyślnie, a wady są istotne – uniemożliwiające prawidłowe korzystanie z oprogramowania i/lub Infrastruktury sprzętowej i/lub Infrastruktury sieciowej Zamawiający może odstąpić od realizacji umowy w całości lub w danej części.
5. Zakończenie testów funkcjonalnych z wynikiem pozytywnym umożliwia odbiór zadania zgodnie z procedurą odbiorową.
6. Testy funkcjonalne zakończą się raportem z testów funkcjonalnych, potwierdzonym przez Zamawiającego bez zastrzeżeń.